Symantec Brightmail AntiSpam™

Version 6.0

Administration Guide

Copyright © 1999–2005 Symantec Corporation. All rights reserved.

Symantec Brightmail AntiSpam
Version 6.0.2
Administration Guide
Document Version 1.0

Brightmail, the Brightmail logo, BLOC, BrightSig, Probe Network and The AntiSpam Leader are trademarks or registered trademarks of Symantec Corporation.

Symantec and the Symantec logo are U.S. registered trademarks and Symantec Security Response (SSR) is a trademark of Symantec Corporation.

Symantec Brightmail AntiSpam is protected under U.S. Patent No. 6,052,709.

See the *Symantec Brightmail AntiSpam Installation Guide* for licenses and notices related to third party software used in Symantec Brightmail AntiSpam.

All other trademarks, service marks, trade names, or company names referenced herein are used for identification only and are the property of their respective owners.

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
U.S.A.
Voice +1 408 517 8000
http://www.symantec.com

Table of Contents

Symantec Brightmail AntiSpam Overview 1
- What's New in Symantec Brightmail AntiSpam 2
- Symantec Brightmail AntiSpam Architecture Overview 3
  - Brightmail Scanner 4
  - Brightmail Control Center 5
- Group Policies, Email Categories and Filtering Actions 6
- Brightmail Filters 8
  - Antispam Filters 8
  - Content Filters 9
  - Blocked and Allowed Senders Lists 9
  - Antivirus Filters 10
- Brightmail Conduit 11
- Brightmail Quarantine 11
- Spam Foldering and Submissions 11

Getting Started with the Brightmail Control Center 13
- Logging In 13
- Logging Out 14
  - Having Trouble Logging In or Out? 14
- Adding Administrators 15

Managing Scanners, Hosts, and Components 19
- About Scanners, Hosts and Components 19
- Setting up Brightmail Scanners 20
  - Adding a Brightmail Scanner 21
  - Testing Brightmail Scanners 24
  - Editing Brightmail Scanners 24
  - Enabling and Disabling Brightmail Scanners 24
  - Deleting Brightmail Scanners 25
- Specifying the SMTP Insertion Host 25

Specifying Internal Mail Hosts 26
Viewing Status of Brightmail Scanners and Components. 29
Starting and Stopping Symantec Brightmail AntiSpam 31

Managing Group Policies. 33
Adding a Group Policy 33
Managing Group Policies 39

Customizing Filtering at Your Site. 41
Specifying Allowed and Blocked Senders 41
About Allowed and Blocked Senders Lists. 42
Reasons to Use Allowed and Blocked Senders. 43
How Brightmail AntiSpam Identifies Senders and Connections 44
Adding Senders to Your Blocked Senders List. 45
Adding Senders to Your Allowed Senders List. 46
Deleting Senders from Lists 47
Editing Senders 47
Enabling or Disabling Senders 47
Importing Sender Information. 48
Exporting Sender Information. 50
Customizing the Brightmail Reputation Service. 50
Adjusting Spam Scoring 51
Enabling Language Identification 53
Adjusting AntiVirus Settings. 54
Available Settings 54
Creating Custom Filters. 56
Using the Custom Filters Editor 56
Importing a Custom Filters File. 64
Details About Custom Filters 64
Sample Custom filters 65

Creating Reports 69
Available Reports 69
Setting the Retention Period for Reporting Data. 72
Choosing Data to Track. 73
Running Reports 73
Troubleshooting Report Generation 74
Understanding the Report Presentation. 75
Saving Reports. 76
Printing Reports. 77

Scheduling Reports 77

Working with Brightmail Quarantine 79
Using LDAP for End User Access to Quarantine 79
Configuring Quarantine for Active Directory 79
Required Exchange 5.5 Settings for Quarantine Compatibility 83
Configuring Quarantine for Exchange 5.5 83
Configuring Quarantine for iPlanet/Sun ONE/Java Directory Server 85
Configuring Quarantine for Other LDAP Servers 88
Working with Messages in Quarantine for Administrators 90
Accessing Quarantine 90
Administrator Message List Page 90
Administrator Message Details Page 93
Searching Messages 94
Working with Messages in Quarantine for End Users 96
Message List Page 96
Message Details Page 98
Searching Messages 99
Configuring Quarantine 101
Delivering Messages to Quarantine from the Brightmail Server . . . 101
Configuring Quarantine for Administrator-Only Access 102
Configuring the User and Distribution List Notification Digests . . . 102
Configuring Recipients for Misidentified Messages 106
Configuring the Delete Unresolved Email Setting 107
Setting the Quarantine Message Retention Period 107
Configuring Messages Per Page in Quarantine 108
Configuring the Login Help 108
Configuring the Quarantine Port for Incoming SMTP Email 109
Specifying Quarantine Message and Size Thresholds 109
Administering Quarantine 110
Starting and Stopping Quarantine 110
Checking the Quarantine Error Log 112
Backing Up the Quarantine Message Database 113
Troubleshooting 113

Monitoring Symantec Brightmail AntiSpam 117
Getting System Status 117
Working with Logs 118
Modifying Log Settings 118
Viewing and Saving Logs 120

Setting Up Event-Based Alerts 121
Periodic System Maintenance 122
Backing Up MySQL Data 122
Maintaining Adequate Disk Space 125
Checking the Status of the MySQL Database 126
Degraded Effectiveness Due to Expired License 126
Checking Versions. 126

Appendix A: Creating Filters by Coding in Sieve 129
Working with the Manually Edited Sieve Filters File. 129
Sieve Implementation Details 130
Sieve Filters File Location. 130
Supported Sieve Commands 130
Sieve Action Commands 131
Sieve Test Commands 132
Sieve Action Precedence 135

Appendix B: Editing Virus Notification Messages 139
Customizing the Cleaner Notification File 139
Cleaner Notification File Listing. 141

Glossary 147

Index 155

Symantec Brightmail AntiSpam Overview

Welcome to Symantec Brightmail® AntiSpam, Symantec's industry-leading message filtering system. Brightmail AntiSpam offers complete, Internet-wide, server-side antispam and antivirus protection. It actively seeks out, identifies, analyzes, and ultimately defuses spam and virus attacks before they inconvenience your users and overwhelm or damage your networks. Symantec software allows you to remove unwanted mail before it reaches your users' inboxes, without violating their privacy.

Brightmail AntiSpam software filters email in four basic ways:

- AntiSpam Filters use our state-of-the-art technologies and strategies to filter and classify email as it enters your site.
- AntiVirus Filters combine Brightmail processing technology with Symantec AntiVirus definitions and engines to clean viruses from your email.
- Content Filters supplement AntiSpam Filters; you can tailor them specifically to the needs of your organization.
- The Allowed Senders List and the Blocked Senders List filter messages based on the sender. You can create your own lists and you can subscribe to third-party lists. As a part of Brightmail AntiSpam, you are automatically subscribed to the Brightmail Reputation Service, which includes our Open Proxy List, Safe List and Suspect List. These lists filter messages based on extensive research to ascertain the reputation of the originating IP address, as a source of spam or of legitimate email.

This section contains the following topics:

- What's New in Symantec Brightmail AntiSpam
- Symantec Brightmail AntiSpam Architecture Overview
- Group Policies, Email Categories and Filtering Actions
- Brightmail Filters
- Brightmail Conduit
- Brightmail Quarantine
- Spam Foldering and Submissions

What's New in Symantec Brightmail AntiSpam

Symantec Brightmail AntiSpam Version 6.0 provides the following enhancements over previous releases:

Table 1. Symantec Brightmail AntiSpam Version 6.0 Enhancements

Feature	Description
Brightmail Control Center	The Brightmail Control Center (Control Center) is a Web-based cross-platform configuration and administration center built in Java. Each Brightmail AntiSpam installation has one Control Center, which also houses Brightmail Quarantine and supporting software. You can configure and monitor all of your Brightmail Scanners from the Control Center. The Control Center replaces the Brightmail configuration file, the Configurator and the Brightmail Administration Console. These components are no longer included in Brightmail AntiSpam.
Brightmail Scanner	Brightmail Scanners perform email filtering. Your Brightmail AntiSpam installation can have one or many Brightmail Scanners. Each Brightmail Scanner includes one or both of the following components: Brightmail Server, Brightmail Client.
Multiple-Machine Management	You can now configure and manage multiple Brightmail Scanners from one Brightmail Control Center. Previously each computer filtering email needed to be configured individually.
Group Policies	You can now specify an unlimited number of user groups, identified by email addresses or domain names, and customize mail filtering for each group. This replaces the previous two-group structure (based on local and foreign domains).
Improved Filtering	Numerous improvements have been made to Brightmail AntiSpam's filtering technologies, including enhanced effectiveness for URL Filters and Heuristic Filters; filtering on mailto: links in messages; improved filtering on MIME headers; and the next generation of Signature Filters, which target comparisons to specific message components with surgical precision.
Brightmail Reputation Service	The Brightmail Reputation Service provides comprehensive reputation tracking that enhances the power of Brightmail AntiSpam. Symantec manages three lists as part of the Brightmail Reputation Service. Each list operates automatically and filters your messages using the same technology as Symantec's other filters. The Brightmail Reputation Service includes the Open Proxy List, the Safe List and the Suspect List.
Improved Reporting	For added convenience and clarity, pre-set reports are now separated into two groups: antispam reports and antivirus reports. You can choose from a selection of reports; each report can be customized to include specific date ranges, time period groupings, and various delivery and output options. For some reports, you can filter based on specific recipients and senders of interest.
Language Identification	Users of the Symantec Plug-in for Outlook can choose from a list of languages in which they would like to receive messages. Messages identified as written in a language not on the user's list will be filtered as spam.
Quarantine Management and End User Improvements	Brightmail Quarantine is now managed via the Brightmail Control Center. You can now set messages to be deleted based on the total size of the Quarantine database or based on each user's storage usage. When users receive digest notifications from Brightmail Quarantine, they can now click on a View link to view an individual message, or click on a Release link to release a message back to the inbox.

Symantec Brightmail AntiSpam Architecture Overview

Using Brightmail AntiSpam, you set up a powerful message filtering system that protects your customers and your network through an approach that is centralized and automated, but also provides customizable, open features that you can tailor for your system. The net effect of this highly scalable structure is to unburden your customers of unwanted email.

As spam messages traverse the Internet, they pass through Symantec's worldwide Probe Network™, an extensive array of email addresses. The Probe Network includes over two million probe accounts that attract the latest spam, based upon up-to-date research into spamming methodologies. The Probe Network sends possible spam emails in real time to the Brightmail Logistics and Operations Center (BLOC™) for evaluation. If the message is verified as spam, the BLOC issues AntiSpam Filters to Brightmail Scanners on your system that isolate similar messages.

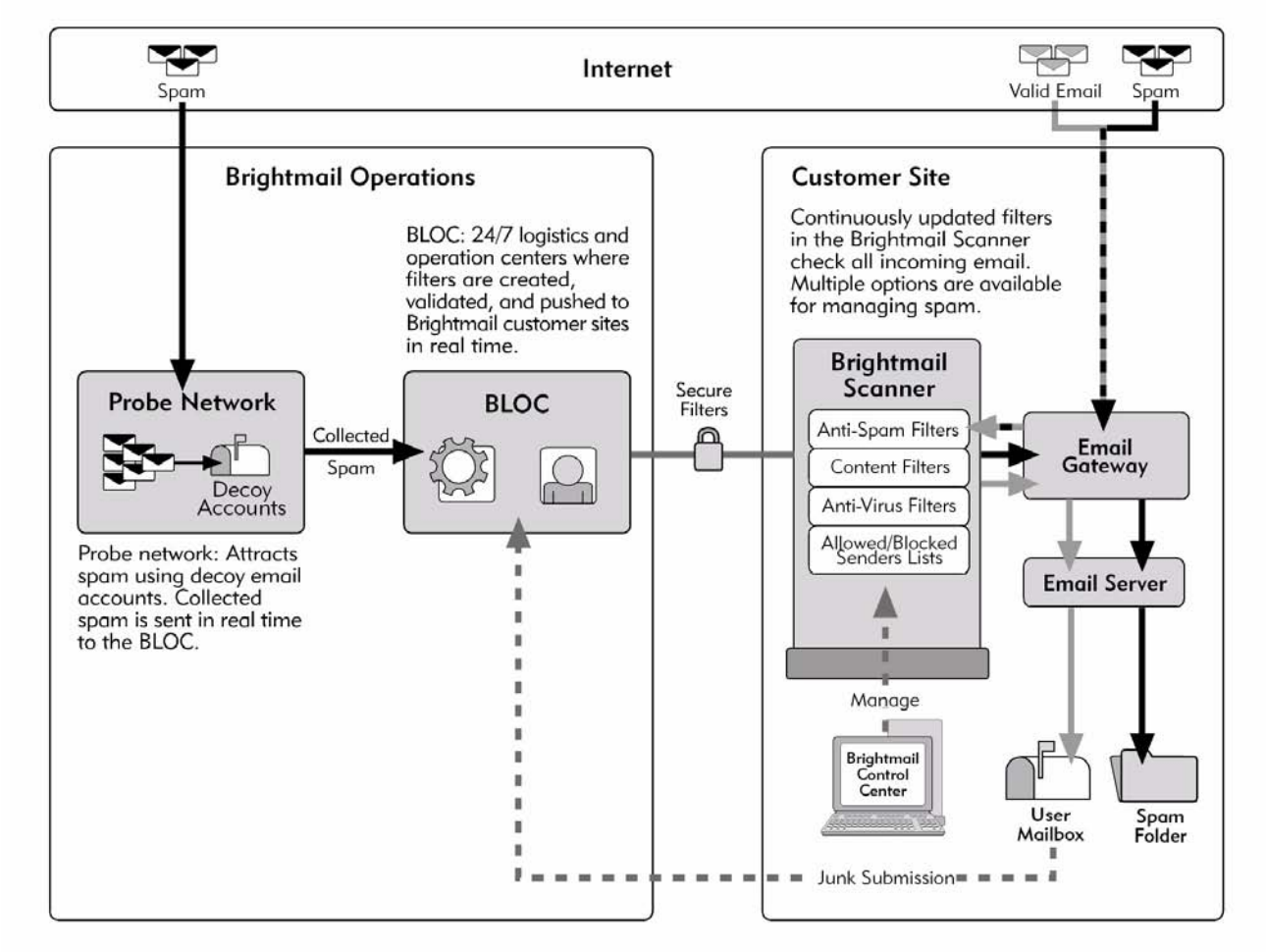
The BLOC consists of several centers working cooperatively on three continents, comprising a round-the-clock protection network that spans the globe. Sophisticated automatic tools, assisted and monitored by BLOC Technicians, evaluate mail for new variations of spam, then issue filters to identify and capture similar messages. The BLOC continuously provides updated filters to Brightmail Servers on your system. BLOC Technicians play an important role in confirming the identification of possible spam. This combination of automation and human intervention allows Symantec Brightmail AntiSpam to adapt in real time to ever-changing spamming techniques, giving it unparalleled flexibility and accuracy as a spam filter.

Most of the filters that the BLOC creates are designed to thwart specific spam attacks. A spam attack can contain thousands of identical or similar messages. By targeting filters against specific attacks, the BLOC keeps Brightmail's false positive rate extremely low (less than 1 in 1,000,000).

Symantec also employs a carefully designed set of heuristic filters, which target patterns common in spam and add a proactive element to our spam-fighting arsenal. Commonly available heuristic filters can lead to large increases in false positives because of the problems inherent in a pattern-matching approach. Brightmail AntiSpam heuristic filters are carefully designed and tested to prevent large increases in false positives.

Figure 1 shows an overview of Symantec Brightmail AntiSpam.

Figure 1. Symantec Brightmail AntiSpam Overview



Brightmail Scanner

Each Brightmail AntiSpam installation can have one or more Brightmail Scanners. Brightmail Scanners perform the actual filtering of email messages.

Each Brightmail Scanner contains:

- A Brightmail Agent
- One or both of the following:
  - A Brightmail Server
  - A Brightmail Client. If the Brightmail Scanner contains a Brightmail Client, then a supported mail transfer agent (MTA) must also reside on the same computer.

Brightmail Agent

This component communicates with the Brightmail Control Center to support centralized configuration and administration activities.

Brightmail Client

The Brightmail Client is a communications channel between the MTA and the Brightmail Server. You can use multiple Brightmail Clients; each one can talk to multiple Brightmail Servers. The Brightmail Client performs load balancing between Brightmail Servers.

Brightmail Server

The Brightmail Servers at your site process spam based on configuration options you select. Each Brightmail Server is a multi-threaded process that listens for requests from Brightmail Clients. Using a variety of state-of-the-art technologies, the Brightmail Server filters messages for classification. The classification, or verdict, is then returned to the Brightmail Client for subsequent delivery action.

Brightmail Control Center

Each Symantec Brightmail AntiSpam installation has exactly one Brightmail Control Center. This is the central nervous system of your Symantec software. The Brightmail Control Center communicates with the Brightmail Agent on each of your Brightmail Scanners. For smaller installations, you can install the Brightmail Control Center and the Brightmail Scanner on the same computer.

From this Web-based graphical user interface, you can:

- Configure, start and stop each of your Brightmail Scanners.
- Specify email filtering options for groups of users or for all of your users at once.
- Monitor consolidated reports and logs for all Brightmail Scanners.
- See summary information.
- Administer Brightmail Quarantine.
- View online help for Brightmail Control Center screens.

The Brightmail Control Center contains the following software:

Brightmail Quarantine

Brightmail Quarantine provides storage of spam messages and Web-based end user access to spam. You can also configure Brightmail Quarantine for administrator-only access. Use of Brightmail Quarantine is optional.

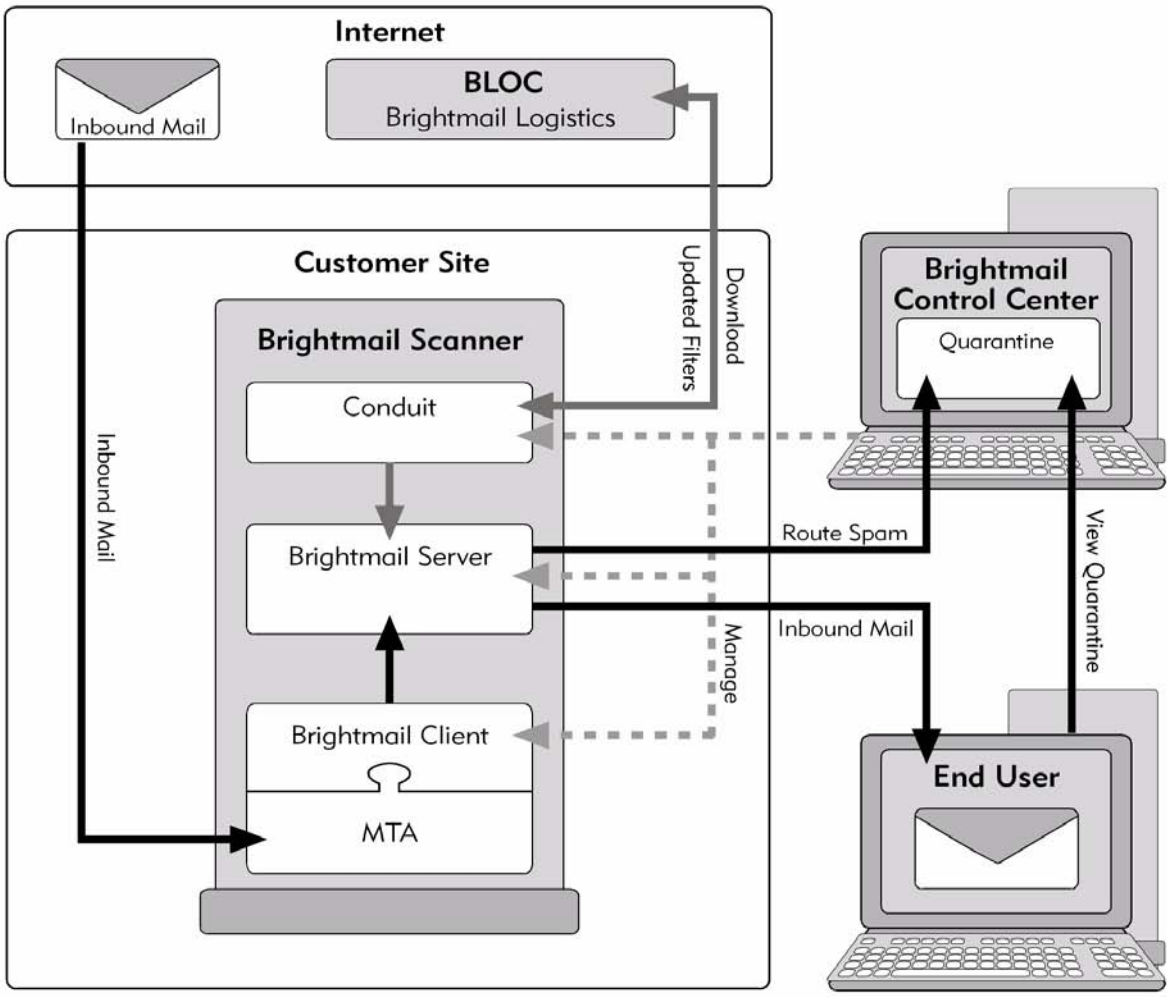
Third Party Software: Database, Web Server

A single MySQL database stores all of your Brightmail AntiSpam configuration information, as well as Brightmail Quarantine information and email messages (if you are using Brightmail Quarantine). Configuration information is communicated to each Brightmail Scanner via an XML file. A Java-based Web Server (by default this is the

Tomcat Web Server) performs Web hosting functions for the Brightmail Control Center and Brightmail Quarantine.

Figure 2 shows the major components of Symantec Brightmail AntiSpam installed at your site.

Figure 2. Symantec Brightmail AntiSpam Components



Group Policies, Email Categories and Filtering Actions

Brightmail AntiSpam provides a wide variety of actions for filtering email, and allows you to either set identical options for all users, or specify different actions for different groups of users.

You can specify groups of users based on email addresses or domain names. For each group, you can specify email filtering actions for seven different categories of email. For each category you can specify one of up to eight different filtering options.

You can choose different filtering actions for the following categories of email:

- **Spam –** Email messages identified as spam using Symantec's AntiSpam Filters.
- **Suspected spam –** You can use Symantec's Spam Scoring to identify a range of email as suspected spam, based on scores assigned by AntiSpam Filters.
- **Email from blocked senders –** You can specify a list of blocked senders, and you can use third party blocked senders lists. The lists included in the Brightmail Reputation Service are used by default.
- **Emails infected with viruses –** Symantec identifies virus-infected messages using AntiVirus Filters, based on Symantec virus definitions and engines.
- **Mass-mailing worms –** Brightmail AntiSpam identifies mass-mailing worm emails as distinct from spam or virus emails, because many customers prefer to delete these emails immediately.
- **Unscannable emails –** These are emails that could not be scanned due to size restrictions or other variables. They may or may not contain viruses. You can choose how to handle these messages.
- **Custom filtered emails –** You can specify special filters unique to your organization, to filter for specific content in email messages.

In addition to the seven categories listed above, you can also specify trusted senders by creating an Allowed Senders List and by subscribing to third party allowed senders lists. Messages from allowed senders are automatically sent to user inboxes, bypassing all filtering (except antivirus filtering, if enabled). The Safe List, part of the Brightmail Reputation Service, is implemented by default.

The filtering actions available vary by email category, and include the following:

- Deliver messages normally.
- Mark messages as spam, either by altering the subject line or by including a configurable X-Header.
- Delete messages.
- Route messages to an administrator's mailbox for subsequent examination.
- Save messages in a directory specified for that purpose.
- Send messages to Brightmail Quarantine, where users can access them via the Web.
- Route messages to each user's spam folder using the Spam Folder Agent, native foldering in Exchange 2003, or Symantec Spam Folder Agent for Domino.
- Clean messages of viruses and deliver each cleaned message normally, with a notification to the recipient.

Brightmail Filters

Brightmail AntiSpam employs the following four major types of filters:

- **AntiSpam Filters –** AntiSpam Filters are created using our state-of-the-art technologies and strategies to filter and classify email as it enters your site.
- **Content Filters –** Custom content filters are written by you, using the Brightmail Control Center or the Sieve scripting language, to tailor filtering to the needs of your organization.
- **Blocked and Allowed Senders Lists –** You can create lists of blocked senders and allowed senders and you can use third party lists. The lists included in the Brightmail Reputation Service are deployed by default.
- **AntiVirus Filters –** Antivirus definitions and engines provided by Symantec protect your users from email-borne viruses.

Antispam Filters

The nature of spam—and the business implications of false positives—demands a careful and flexible approach to filter creation. Accordingly, Symantec does not use a one-size-fits-all approach to creating filters. Instead, it employs a combination of filtering strategies, based on the specific type of spam. Some technologies perform sophisticated comparisons with the latest spam received by the Probe Network, resulting in matches of unparalleled accuracy. Others are more proactive, attacking future spam based on special characteristics or origination information. Symantec filter types include:

- Heuristic Filters
- URL Filters
- Signature Filters
- Header Filters

Heuristic Filters – Heuristic Filters scan the headers and the body of a message, applying a variety of tests. These tests search for tell-tale characteristics that are usually inherent in spam, such as opt-out links, specific phrases, and forged headers. Each characteristic is assigned a spam probability, and the message is given a cumulative probability score based on the overall test results. If a certain probability threshold is reached, Brightmail AntiSpam determines the message to be spam. Using heuristics, Brightmail AntiSpam software can make the determination that a message is spam, even if it hasn't passed through the Probe Network. The BLOC transmits updated Heuristic Filters as it does other AntiSpam Filters.

URL Filters – Symantec's URL Filters catch messages based on specific URLs found in spam. URL-based spam is increasingly pervasive because spammers want to direct readers to a specific Web site for contact information or purchasing instructions. Although the underlying URLs do not change frequently, spammers attempt to obfuscate and disguise them. As a result, these URLs appear to be unique across similar spam messages.

Signature Filters – When messages flow into the BLOC, they are characterized using proprietary algorithms into a unique *signature*, which is added to the database of known spam. Using this signature, Signature Filters group and match seemingly random messages that originated from a single attack. By distilling a complex and evolving attack to its DNA, more spam can be deflected with a single filter. Signature Filters include BrightSig2 Filters, Body Hash Filters and Attachment Filters.

Header Filters – Header Filters are regular expression-based filters that are applied to the header lines of a message. Header Filters can be used to compare email messages to spam messages seen by the Probe Network, and to exploit commonalities or trends present in spam messages (similar to the use of Symantec's Heuristic Filters).

Content Filters

You can create custom content filters, using either the Custom Filters Editor provided through the Brightmail Control Center, or using a Sieve filters file. You can specify a wide variety of filtering criteria. You have three sets of choices for the action to take on these messages:

- Deliver normally.
- Treat the same as another email category: You can use the same action on custom-filtered messages that you chose for spam, viruses, or any other category.
- Treat as company-specific content: Choose a unique action for custom-filtered messages.

Blocked and Allowed Senders Lists

You can use lists of blocked and allowed senders (also known as *blacklists* and *whitelists*) in a variety of ways:

- **Define a custom Allowed Senders List –** Allowed senders are approved or trusted senders. Unless AntiVirus Filters detect a virus or worm, Brightmail AntiSpam always treats mail coming from an address or connection in your Allowed Senders List as legitimate mail. Such mail is delivered immediately to the inbox, bypassing any other filtering. You therefore cannot choose message handling actions for messages from allowed senders; by definition these messages will be delivered to the user inbox.
- **Define a custom Blocked Senders List –** You can block messages from any senders you wish. You can define message handling actions that apply to messages from blocked senders for each group policy.
- **Check incoming mail against third party blocked senders lists and third party allowed senders lists –** Third parties compile and manage lists of desirable or undesirable domains, IP connections, and networks. A *DNS blacklist* is a common example of such a list. DNS blacklists allow subscribers to check, using DNS lookups, whether incoming mail is originating from known spammers. Many of the hosts on the list typically are running open SMTP relays or open proxy server ports. Such insecure relays and ports are effective conduits for sending unsolicited bulk email. Subscribers to DNS lists can thus block or delete mail from these blacklisted hosts. On the other

hand, administrators who subscribe to *DNS whitelists* can leverage a list of legitimate mail servers and senders. You can add a DNS blacklist as a third party blocked senders list. You can add a DNS whitelist as a third party allowed senders list.

- **Brightmail Reputation Service Lists:** By default, Brightmail AntiSpam is configured to check mail against three lists, all part of the Brightmail Reputation Service, managed by Brightmail. Unlike other lists, which simply aggregate information and are frequently outdated, the Brightmail Reputation Service lists are generated and updated hourly. They are downloaded to your system and updated just like other filters.
  - The **Open Proxy List** is a dynamic database containing IP addresses of identity-masking relays, including proxy servers with open or insecure ports. Because open proxy servers allow spammers to conceal their identities and off-load the cost of emailing to other parties, spammers will continually misuse a vulnerable server until it is brought offline or secured. Brightmail recommends that organizations secure their proxy servers to ensure that spammers cannot connect to open ports and relay SMTP email.
  - The **Safe List** is a list of IP addresses from which virtually no outgoing email is spam.
  - The **Suspect List** is a list of IP addresses from which virtually all of the outgoing email is spam.

Antivirus Filters

NOTE: *The following information and all other references to antivirus functions assume you have purchased antivirus filtering offered by Symantec for Brightmail AntiSpam.*

Virus experts at Symantec Security Response (SSR) provide up-to-date virus definitions and engines to rid email attachments of unwanted viruses.

The BLOC, through automated processes monitored by BLOC Technicians, integrates the virus definitions and engines into AntiVirus Filters, tests them, and distributes them to your site.

The Brightmail Scanner, using the AntiVirus Cleaner (Cleaner), filters the attachments of incoming email in search of viruses. If filtering detects no viruses, the message is analyzed for spam. If filtering detects one or more viruses, the policies you have set up go into effect. For example, you can instruct the Brightmail Scanner to delete the message or to clean and then deliver the message. You can also set policies potential virus messages that cannot be processed by the Cleaner.

Brightmail AntiSpam also provides protection against mass-mailing worms, which can leave hundreds of spam messages in their wake. The Worm Auto-Delete feature automatically removes not only the worm but also the associated messages. This convenient feature saves users from having to wade through hundreds of inbox messages that, although clean from viruses, serves no valuable purpose.

If the Cleaner finds an infected message, it sends an advisory message to the intended recipient. This configurable message informs the recipient that the infected attachment has been cleaned, deleted, or delivered without cleaning. The Cleaner inserts the original message, if delivered, as an attachment to the advisory message. The Cleaner also places a special identifying line in the message header so that the message is not filtered again for viruses.

Brightmail Conduit

Having up-to-date filters is imperative to ensure the highest success rate of filtering and blocking unwanted email. Filter updates are accomplished through a dialogue between the BLOC and the Brightmail Conduit, a Brightmail AntiSpam component that runs at your site. The Conduit handles all such communication at your site. The Conduit runs on each Brightmail Scanner that contains a Brightmail Server.

The Conduit polls a secure Web site every minute to check for the availability of new filters from the BLOC. If new filters are available, the Conduit retrieves the updated filters using secure HTTPS file transfer. After authenticating the filters, the Conduit notifies the Brightmail Server to begin using the updated filters. The Conduit also manages statistics, both for use by the BLOC and by the Brightmail Control Center, which aggregates the statistics from Brightmail Scanners to create consolidated reports.

Brightmail Quarantine

Brightmail Quarantine (Quarantine) provides users direct Web-based access to spam messages that Brightmail software has sidelined into the Quarantine database for them. Users can check for misidentified messages, resend messages to their inbox, and delete or search messages. An administrator account provides access to all quarantined messages.

Quarantine stores spam messages in the Brightmail AntiSpam MySQL database on the Brightmail Control Center computer. A Notifier process periodically sends users a reminder to check their spam messages in Quarantine. Spam messages older than a customizable time period are deleted automatically by an Expunger process. A Java-based Web Server presents the Quarantine interface to users.

Spam Foldering and Submissions

Brightmail AntiSpam features the Spam Folder Agent and Symantec Spam Folder Agent for Domino, designed to work on Microsoft Exchange and Lotus Domino Servers, respectively. Installed separately from the standard Brightmail installation, these agents create a subfolder and a server-side filter in each user’s mailbox. This filter gets applied to messages that the Brightmail Scanner identifies as spam, routing spam into each user’s spam folder. The spam folder agents relieve end users and administrators of the burden of

using their mail clients to create filters. The Symantec Spam Folder Agent for Domino also allows users to submit missed spam and false positives to Symantec.

The Symantec Plug-in for Outlook makes it easy for Outlook users to submit missed spam and false positives to Brightmail. Depending on how you configure the plug-in, user submissions can also be sent automatically to a local system administrator. The Symantec Plug-in for Outlook also gives users the option to administer their own allowed senders and blocked senders lists.

Getting Started with the Brightmail Control Center

This section tells you how to begin using the Brightmail Control Center and describes the user interface at a high level. The following topics are covered here:

- Logging In
- Logging Out
- Adding Administrators

Logging In

Follow these instructions to begin using the Brightmail Control Center. If you are unsure which scenario applies to you, contact your system administrator.

If you are a new administrative user:

1. In the **Login as** box, type `admin`.
2. In the **Password** box, type the default password. Contact your system administrator if you do not know the password.
3. Click **Login**.

If you have an account on an iPlanet, Sun ONE, or Java Directory Server:

1. In the **Login as** box, type your full email address (for example, `kris@corp.com`).
2. In the **Password** box, type the password you normally use to log in to your system.
3. Click **Login**.

If you have an Active Directory account:

1. In the **Login as** box, type your user name (for example, `kris`).
2. In the **Password** box, type the password you normally use to log in to your system.
3. Select the LDAP server you use to verify your credentials (not shown).
4. Click **Login**.

If you have an Exchange 5.5 account:

1. In the **Login as** box, type your full primary email address (for example, `kris@corp.com`).
2. In the **Password** box, type the password you normally use to log in to your Windows system.
3. Click **Login**.

To determine your primary email address for Exchange 5.5, check the following in Outlook 2000 or Outlook 2003:

1. Click **Tools**, click **Address Book**.
2. Type your name in the **Type Name or Select from List** box.
3. Double-click your name in the list displayed, and then click **E-mail Addresses**.
4. The mail address on the line starting with `SMTP:` in capitals is your primary email address.

Logging Out

1. Click the **Log Out** icon

in the upper right corner of the current page.
2. For security purposes, close your browser window to clear your browser's memory.

Having Trouble Logging In or Out?

- When logging in, make sure you type your user name and password in the correct case. Note the difference between `kris`, `Kris`, and `KRIS`.
- You are automatically logged out if you don't use the Brightmail Control Center for a certain period (usually 30 minutes). If that happens, log in again.
- If you see an error message similar to the following, you've attempted to log in as an administrator without sufficient privileges to add a Brightmail Scanner on a system with no configured Brightmail Scanners. You must add a Brightmail Scanner in the Brightmail Control Center to access the rest of the Control Center, and only an administrator with full privileges can add a Brightmail Scanner. To enable access for administrators without full privileges, log in as an administrator with full privileges and configure a Brightmail Scanner.

```
The system configuration is incomplete. An administrator with full
   privileges must add a Scanner first.
```

Adding Administrators

You can create additional administrator accounts, granting each administrator the desired level of management privileges for different components of Brightmail AntiSpam. For example, you might want to delegate management of Quarantine to another administrator, who will only be able to modify Quarantine settings.

When granting an administrator limited privileges, you can assign any or all of the following management actions:

- Manage Quarantine
- Manage Status and Logs
- Manage Reports
- Manage Group Policies

The available tabs and settings in the Brightmail Control Center change dynamically depending on your level of administrator privileges. Once you log on as an administrator, you will only see the tabs pertinent to your management privileges. The page samples in this document assume that you have full administrative privileges.

NOTE: *Only administrators with full privileges can create a new administrator account.*

The following sets of privileges apply to the specified administrator levels:

Full Administrative Privileges

- Access to the Summary Tab
- Access to the Status Tab
- Access to the Reports Tab
- Access to the Logs Tab
- Access to the Quarantine Tab
- Access to all links on the Settings Tab

Limited Privileges: Manage Quarantine

- Access to the Quarantine Tab.
- Access to the Settings Tab with the following links only:
  - Administrators
  - LDAP
  - Quarantine

Limited Privileges: Manage Status and Logs

- Access to the Summary Tab
- Access to the Status Tab
- Access to the Logs Tab
- Access to the Settings Tab with the following links only:

— Administrators
— Logs

Limited Privileges: Manage Reports

- Access to the Reports Tab
- Access to the Settings Tab with the following links only:
  — Administrators
  — Reports

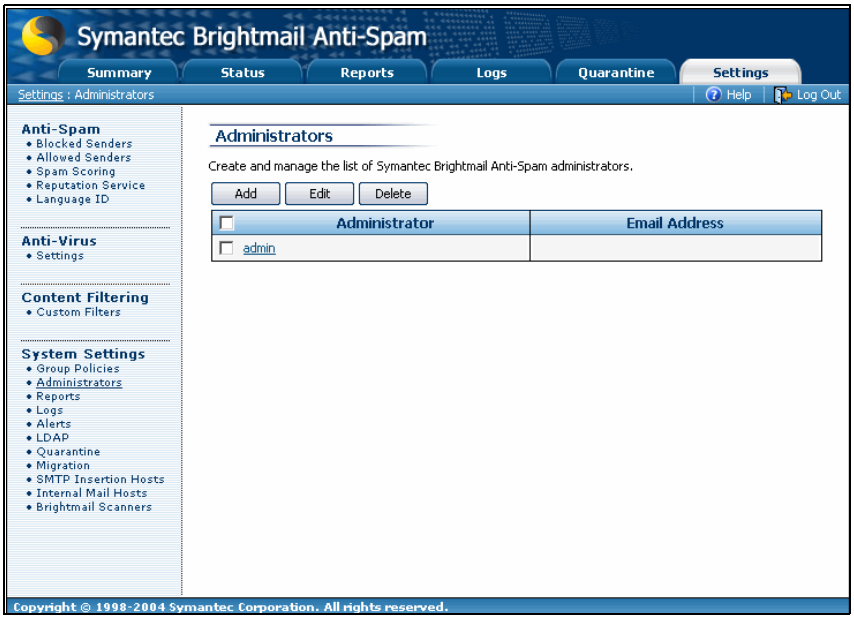
Limited Privileges: Manage Group Policies

- Access to the Settings Tab with the following links only:
  — Administrators
  — Group Policies

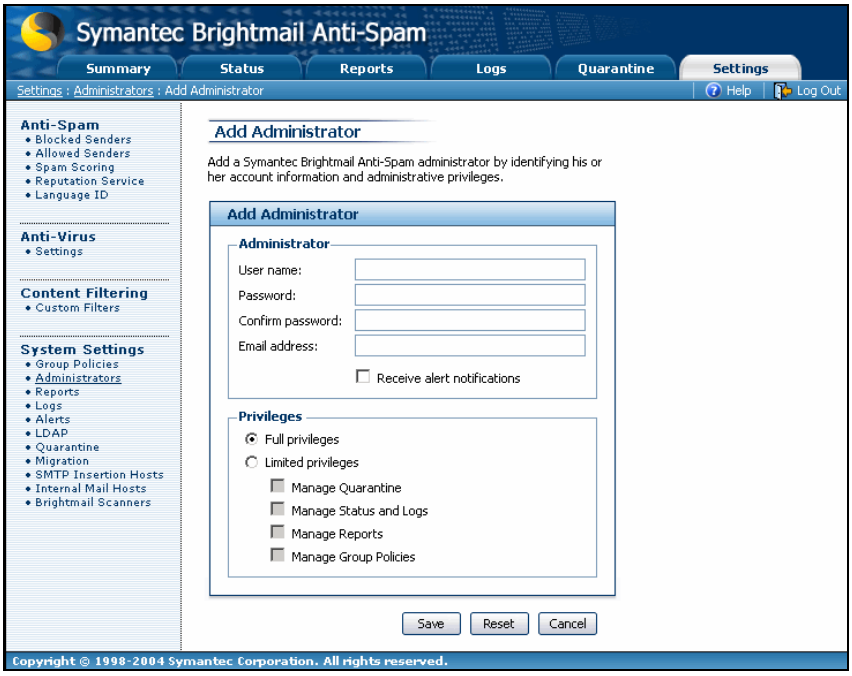
To add an administrator:

1 In the Brightmail Control Center, click the **Settings** tab.

2 In the left pane, under **System Settings**, click **Administrators**.
The Administrators page is displayed.



3 Click **Add**.
The Add Administrator page is displayed.



4 Under **Administrator**, fill in the information about the administrator you want to add.

5 Select the **Receive alert notifications** check box if applicable.

If you select this check box, Brightmail AntiSpam will email the administrator if error conditions arise with Brightmail AntiSpam components. You can define these error conditions in the **Alerts** page on the **Settings** tab.

6 Under **Privileges**, do one of the following:

— To add an administrator with access to all available Brightmail Control Center settings, click **Full Privileges**.

— To add an administrator with limited access, click **Limited Privileges** and clear or select check boxes based on the desired management role.

7 Click **Save**.

Managing Scanners, Hosts, and Components

This section describes how to use the Brightmail Control Center to set up and manage the necessary hosts and components so that Symantec Brightmail AntiSpam works properly in your environment.

This section includes the following topics:

- About Scanners, Hosts and Components
- Setting up Brightmail Scanners
- Specifying the SMTP Insertion Host
- Specifying Internal Mail Hosts
- Viewing Status of Brightmail Scanners and Components
- Starting and Stopping Symantec Brightmail AntiSpam

About Scanners, Hosts and Components

There are two general classifications of computers that run Brightmail software: Brightmail Control Centers and Brightmail Scanners. These designations can be logical or physical, depending on the specific software you installed on each host. For example, you can install Brightmail Control Center software and Brightmail Scanner software on the same computer. In such a case, the computer you use will become both your Brightmail Control Center and a Brightmail Scanner.

The following table describes the main differences between the Control Center and the Scanners.

Table 2. Brightmail Control Centers and Brightmail Scanners

	Control Center	Brightmail Scanner
Description	Host to which administrators connect using a Web browser for centralized management of other computers that are running Symantec Brightmail AntiSpam software. Also provides the infrastructure for central Web-based Brightmail Quarantine.	Host that is responsible for interacting with the MTA and providing filtering services.
Required Components	Brightmail Control Center	Brightmail Agent Brightmail Client and/or Brightmail Server The following supporting components have minimal setup requirements and are only present on Brightmail Scanners that include a Brightmail Server: • Conduit • AntiVirus (no initial setup required) • Harvester (no initial setup required)
Available Components	Brightmail Quarantine	N/A
Configuration Information	Brightmail Control Center: See *Symantec Brightmail AntiSpam Installation Guide*. Brightmail Quarantine: see "Working with Brightmail Quarantine," on page 79	See this chapter.

In addition to setting up Brightmail-specific hosts, you also need to provide information about other hosts. For example, you need to identify the computer that will reinsert messages. Also, if you're not deploying all Brightmail Scanners at the gateway, you need to identify all internal mail servers that process mail in order for connection filtering for your Allowed Senders List and Blocked Senders List to work.

Setting up Brightmail Scanners

Use the **Brightmail Scanners** page to set up Brightmail Scanners. This section includes the following topics:

- Adding a Brightmail Scanner
- Testing Brightmail Scanners
- Editing Brightmail Scanners

- Enabling and Disabling Brightmail Scanners
- Deleting Brightmail Scanners

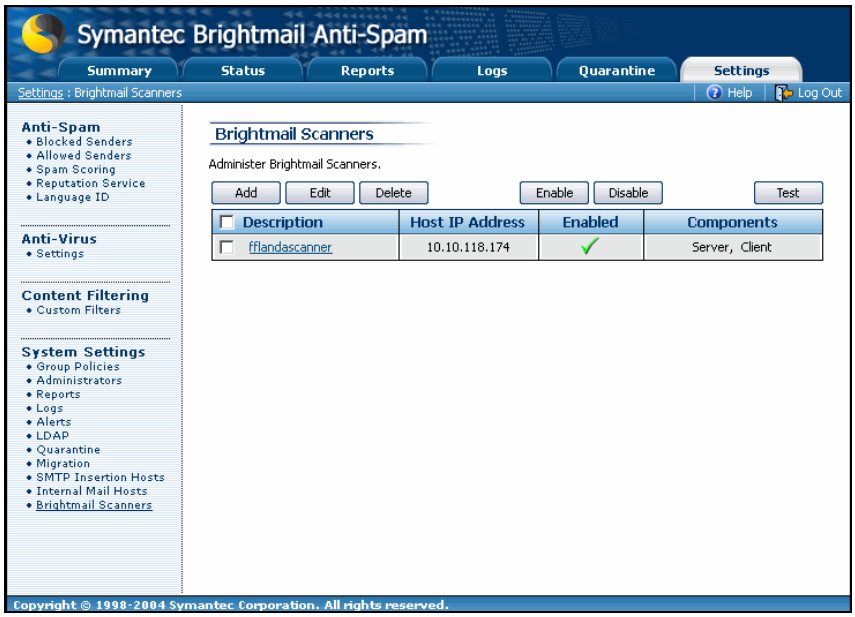
Adding a Brightmail Scanner

Step 1: Define the Initial Host Configuration

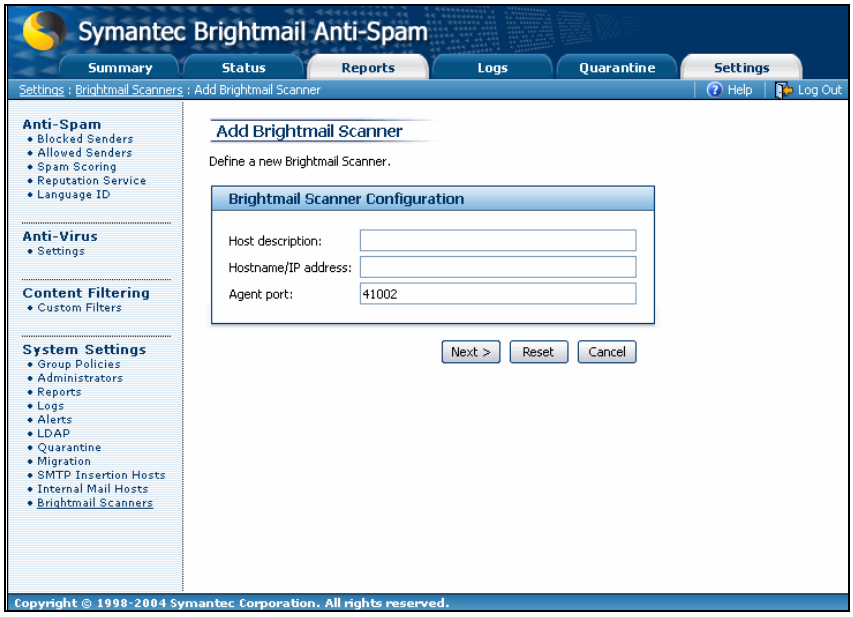
Specify the host's IP address and the port used by the Brightmail Agent.

To set up a Brightmail Scanner:

1. In the Brightmail Control Center, click the **Settings** tab.
2. In the left pane, under **System Settings**, click **Brightmail Scanners**.
   The Brightmail Scanners page is displayed.



3. Click **Add**.
   The Add Brightmail Scanner page is displayed.



4 In the **Host description** box, specify a name for the Brightmail Scanner.

5 In the **Hostname/IP address** box, specify the fully qualified hostname or IP address for the Brightmail Scanner you want to add.

6 In the **Agent port** box, accept the default port used by the Brightmail Agent.

NOTE: *Do not change the* **Agent port** *value.*

7 Click **Next**.

Step 2: Choose the Required Components

In the next stage of Brightmail Scanner configuration, you decide which components you want to enable and configure. The two components you can choose to enable are the Brightmail Client and the Brightmail Server. You can enable one or both of these components.

To specify the components to enable on a Brightmail Scanner:

1 After adding a Brightmail Scanner, check the components you want to enable.

2 Click **Configure** next to the component you want to configure.

3 Go to "Step 3: Configure Brightmail Servers" and/or "Step 4: Configure Brightmail Clients" depending on your choice.

Step 3: Configure Brightmail Servers

Configuring a Brightmail Server consists of the following tasks:

- **Specify the port used by the Brightmail Server –** In order for the Brightmail Client and the Brightmail Server to communicate with each other, the correct port must be

provided. You need to provide the network address of the machine running the Brightmail Server.

- **Specify optional proxy server configuration for the Conduit –** The Conduit enables secure HTTPS transmission of filter updates sent from the BLOC to your Brightmail Scanner. It also sends statistics information from your Brightmail Scanners to the BLOC. The Conduit is pre-configured to connect to the necessary URLs for a given rule type or to the BLOC for statistics transmissions. If your site requires a proxy server for HTTPS Web access, you must specify it.

To configure the Brightmail Server:

1. Choose to configure the Brightmail Server as described above.
2. On the **Configure Brightmail Server** page, type the port number on which the Brightmail Server listens for Brightmail Client connections. Only one port can be specified per server.
3. If you need to configure a proxy server for the Conduit, do the following:
   a. Click **Use a proxy server to receive filter updates**.
      Additional boxes for proxy server identification and authentication become available.
   b. In the **Address** box, type the address for your proxy server. Typically, this is specified as a server name or IP address.
   c. In the **Port** box, specify the port being used by your proxy server.
   d. In the **User name** box, type your user ID for authentication, if required.
   e. In the **Password** box, type your password, if required. It will not be displayed on the page when entered.
4. Click **Save**.
5. Go to "Step 4: Configure Brightmail Clients" if you want to configure the Brightmail Client. Otherwise, if you are finished with this Brightmail Scanner, click **Save**.

Step 4: Configure Brightmail Clients

Configuring the Brightmail Client involves specifying the available Brightmail Servers to which clients can connect.

To set up Brightmail Server connections for Brightmail Clients:

1. Choose to configure the Brightmail Client as described in "Step 2: Choose the Required Components".
2. Do one of the following:
   — To add a Brightmail Server, select a server from the **Available Brightmail Servers** section, and then click **Add**.
   — To prevent a Brightmail Server from receiving client connections, select a server from the **Connected Brightmail Servers** section, and then click **Remove**.

Testing Brightmail Scanners

Once you add a Brightmail Scanner, you can quickly test whether the Brightmail Scanner is up and whether the Brightmail Agent is able to make a connection.

To test a Brightmail Scanner:

1. In the Brightmail Control Center, click the **Settings** tab.
2. In the left pane, under **System Settings**, click **Brightmail Scanners.**
3. On the **Brightmail Scanners** page, select the hosts you want to test, and then click **Test**.

   If the test is successful, Brightmail AntiSpam displays feedback at the top of the page.

Editing Brightmail Scanners

Once you set up a Brightmail Scanner, you can go back and edit the configuration. For example, you can change the host IP address or enable different components.

To edit a Brightmail Scanner:

1. In the Brightmail Control Center, click the **Settings** tab.
2. In the left pane, under **System Settings**, click **Brightmail Scanners**.
3. On the **Brightmail Scanners** page, select the host that you want to edit, and then click **Edit**.

NOTE: *You can also click the underlined description of a Brightmail Scanner to jump directly to the **Edit Brightmail Scanner** page.*

4. Make any changes to host or included components.
5. When you are finished making changes, click **Save**.

Enabling and Disabling Brightmail Scanners

For troubleshooting or testing purposes, you might need to disable and then re-enable Brightmail Scanners. Also, before deleting a Brightmail Scanner, you must disable it first. A disabled Brightmail Scanner will not process mail.

To enable or disable a Brightmail Scanner:

1. In the Brightmail Control Center, click the **Settings** tab.
2. In the left pane, under **System Settings**, click **Brightmail Scanners.**

   A red x (✗) in the Enabled column indicates that the Brightmail Scanner is disabled.

   A green check mark (✓) in the Enabled column indicates that the Brightmail Scanner is enabled.
3. In the list of available Brightmail Scanners, do one of the following:

— To enable a Brightmail Scanner that is currently disabled, select it, and then click **Enable**.

— To disable a Brightmail Scanner that is currently enabled, select it, and then click **Disable**.

The list updates to reflect your choice.

Deleting Brightmail Scanners

When you delete Brightmail Scanners using the Brightmail Control Center, you do not physically remove Brightmail Scanner software—you only remove the specific Brightmail Scanner definition from the Brightmail Control Center database. To prevent a Brightmail Scanner from continuing to run after you delete the definition, make sure you disable it before deleting it. See "Enabling and Disabling Brightmail Scanners," on page 24 for instructions.

To delete a Brightmail Scanner:

1. In the Brightmail Control Center, click the **Settings** tab.
2. In the left pane, under **System Settings**, click **Brightmail Scanners.**
3. On the **Brightmail Scanners** page, click the check box corresponding to the host that you want to delete, and then click **Delete**.

   The host is removed from the list of available Brightmail Scanners.

Specifying the SMTP Insertion Host

During the filtering process, Brightmail AntiSpam must periodically remove a message from the mail flow, modify it, and then reinsert it back into the mail stream for delivery. Brightmail AntiSpam also generates messages, such as email notifications and message quarantine digests, that must be sent unfiltered to administrators and end users.

Note the following when specifying an Insertion Host:

- **Supported syntax –** Specify an IP address or hostname (e.g. `192.9.9.12` or `smtp.example.com`). Specify `127.0.0.1` to use the current computer.
- **Optional Insertion Host specific to antivirus operations –** Brightmail AntiSpam diverts messages containing known viruses through a virus cleaner, then re-inserts them into the mail stream. During this process, if the virus can be isolated from the mail message, it is removed. Otherwise, all message content is stripped and replaced with text notifying the recipient of the fact.

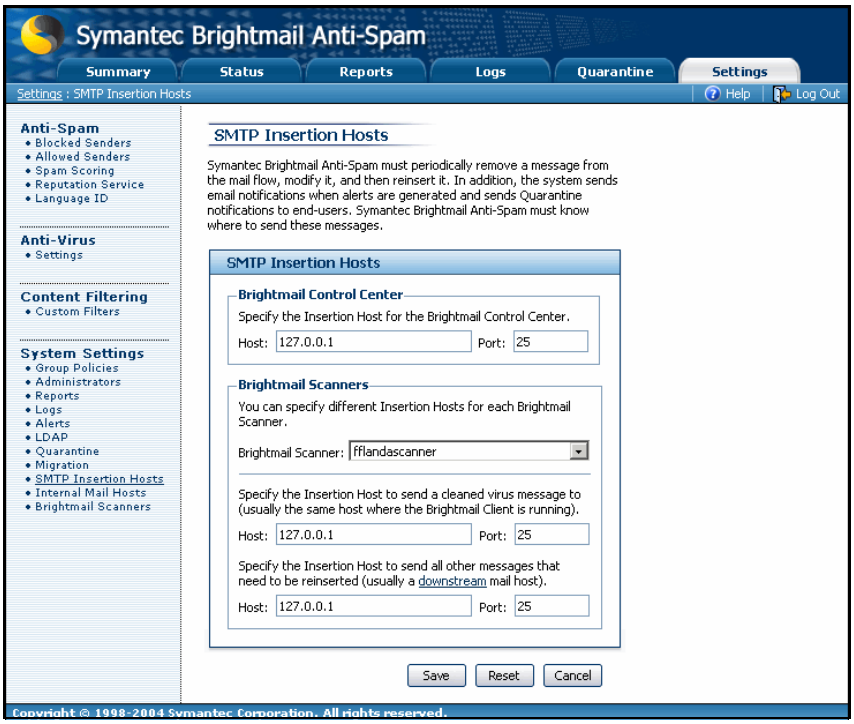
  You can specify one insertion host for cleaned messages and another Insertion Host for all other messages.

To specify the Insertion Host for a Brightmail Scanner:

1. In the Brightmail Control Center, click the **Settings** tab.

2 In the left pane, under **System Settings**, click **SMTP Insertion Hosts**.

The SMTP Insertion Hosts page is displayed.


Symantec Brightmail Anti-Spam
Summary
Status
Reports
Logs
Quarantine
Settings
Settings : SMTP Insertion Hosts
Help
Log Out
Anti-Spam
• Blocked Senders
• Allowed Senders
• Spam Scoring
• Reputation Service
• Language ID
Anti-Virus
• Settings
Content Filtering
• Custom Filters
System Settings
• Group Policies
• Administrators
• Reports
• Logs
• Alerts
• LDAP
• Quarantine
• Migration
• SMTP Insertion Hosts
• Internal Mail Hosts
• Brightmail Scanners
SMTP Insertion Hosts
Symantec Brightmail Anti-Spam must periodically remove a message from the mail flow, modify it, and then reinsert it. In addition, the system sends email notifications when alerts are generated and sends Quarantine notifications to end-users. Symantec Brightmail Anti-Spam must know where to send these messages.
SMTP Insertion Hosts
Brightmail Control Center
Specify the Insertion Host for the Brightmail Control Center.
Host: 127.0.0.1 Port: 25
Brightmail Scanners
You can specify different Insertion Hosts for each Brightmail Scanner.
Brightmail Scanner: fflandascanner
Specify the Insertion Host to send a cleaned virus message to (usually the same host where the Brightmail Client is running).
Host: 127.0.0.1 Port: 25
Specify the Insertion Host to send all other messages that need to be reinserted (usually a downstream mail host).
Host: 127.0.0.1 Port: 25
Save
Reset
Cancel
Copyright © 1998-2004 Symantec Corporation. All rights reserved.

3 Under **Brightmail Control Center**, use the **Host** and **Port** boxes to identify the SMTP server that the Brightmail Control Center will use. This server is used to send the following types of messages:

— Messages released to the inbox by Quarantine users

— Alerts

— Reports

4 In the **Brightmail Scanner** list, select a Brightmail Scanner.

5 Use the next set of **Host** and **Port** boxes to identify the SMTP server that will deliver messages cleaned by Brightmail AntiSpam.

6 In the following **Host** and **Port** boxes, specify the insertion host that will deliver all other reinserted messages.

7 Click **Save**.

Specifying Internal Mail Hosts

NOTE: *Disregard this section if all your Brightmail Scanners are deployed at the gateway.*

To provide accurate source-based filtering for the Allowed Senders List and the Blocked Senders List, Brightmail AntiSpam needs to know which IP addresses are internal to your organization and which are external. Internal servers are typically internal relay or mailbox servers located downstream from the gateway servers. A gateway server is usually deployed at or near the Internet and accepts incoming Internet email messages and forwards these messages to the appropriate internal mailbox servers.

If you are deploying Brightmail AntiSpam anywhere else but at the gateway, you need to provide information about your internal mail or MX network. With this information, Brightmail AntiSpam can extract a message's logical connection address, which is the connection address obtained where the message entered your network. In non-gateway deployments, Brightmail AntiSpam uses this logical connection to match against IP connections specified on your Allowed Senders List, Blocked Senders List, or the Safe List provided by the Brightmail Reputation Service.

Note the following about internal mail hosts:

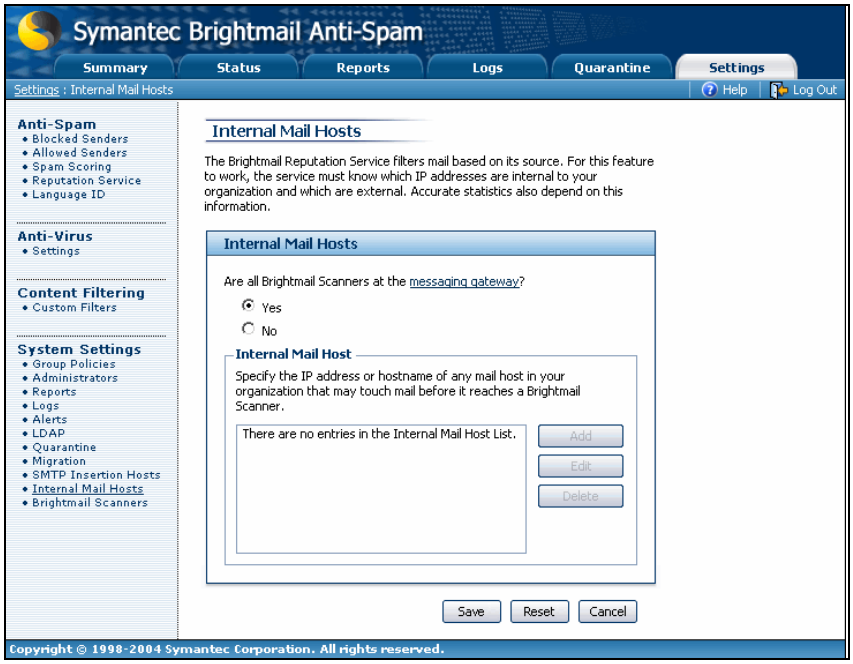
- Brightmail AntiSpam bases its view of your network on the specified internal address ranges and on the received headers remaining intact between the edge of your network and the computers on which the Brightmail Scanners are deployed.
- If you choose to provide a hostname when identifying an internal host, ensure that the hostname resolves to a single address.
- The process of using internal mail hosts settings to extract logical connections applies only to the Blocked Senders List, the Allowed Senders Lists, and the Safe List. It does not apply for reporting, custom filters, or other features in Brightmail AntiSpam that make use of IP connection addresses. In the latter cases, you should deploy Brightmail AntiSpam at the gateway if you want receive the most complete information about IP addresses.
- You do not need to specify any private address space (for example, `10.0.0.0/8` or other subnets defined as private in RFC 1918) in the internal address range, because these are automatically incorporated into the internal address range.

NOTE: *Instead of only identifying the address range for your MX/mail network, you can add your entire internal network range in one step (x.y.z.0/24). With this method, if you ever add new mail servers, new networks, or add IP addresses to your network, you don't need to adjust the settings on this page. If you choose this method, the Brightmail Reputation Service will not apply to these addresses. (The consequences of this are minimal, because the addresses are from your own network).*

To specify the addresses for internal mail hosts:

1. In the Brightmail Control Center, click the **Settings** tab.
2. In the left pane, under **System Settings**, click **Internal Mail Hosts**.

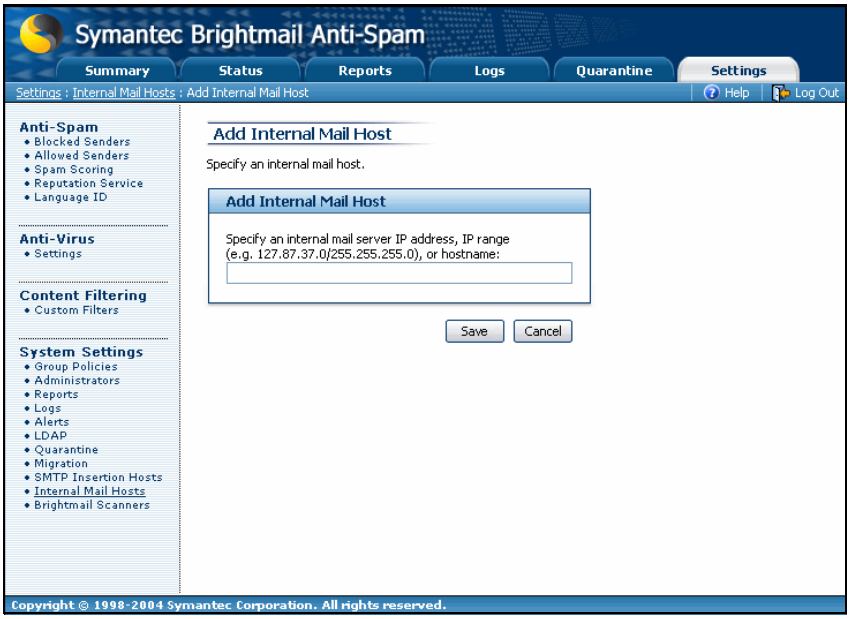
   The Internal Mail Hosts page is displayed.



3 Because one or more Brightmail Scanners are deployed on non-gateway mail servers, click **No**.

4 Click **Add**.

The Add Internal Mail Host page is displayed.



5 On the **Add Internal Mail Host** page, identify the mail server. You can provide the hostname, IP address, or IP range.

Do not specify hostnames which DNS resolves to multiple addresses or to a randomly selected address.

6 Click **Save**.

The list of hosts on the Internal Mail Hosts page refreshes.

7 Do one of the following:

— To edit an internal mail host, select the host, and then click **Edit**. Make any changes, and then click **Save**.

— To remove an internal mail host from the list, select the host, and then click **Delete**.

— If you are finished working with the list of internal mail hosts, click **Save**.

Viewing Status of Brightmail Scanners and Components

You can view more detailed status for all your configured Brightmail Scanners and for Brightmail Quarantine from one central location on the Brightmail Control Center. You can also selectively stop and start components and Brightmail Scanners from this page.

The **Status** page lists:

- Quarantine information (if you are using Brightmail Quarantine)
- The configured Brightmail Scanners in your network
- The associated components for each Brightmail Scanner
- The basic status (running or not) of the hosts and components

The following table summarizes the additional status information that the **Status** page provides for larger components:

Table 3. Status Information for Brightmail Scanners and Components

Item	Component Description	Additional Status Information Provided
Scanner	Brightmail Scanner controlled by the Control Center.	N/A
Server	Brightmail Server residing on the Brightmail Scanner.	Per-server filtering statistics
Conduit	Downloads updated filters from Brightmail.	Date and time of last set of successful filter downloads
Agent	Communicates with the Brightmail Control Center to support centralized configuration and administration activities via the Brightmail Control Center.	N/A
Client	Brightmail Client that integrates with the MTA and interacts with the Brightmail Server.	N/A

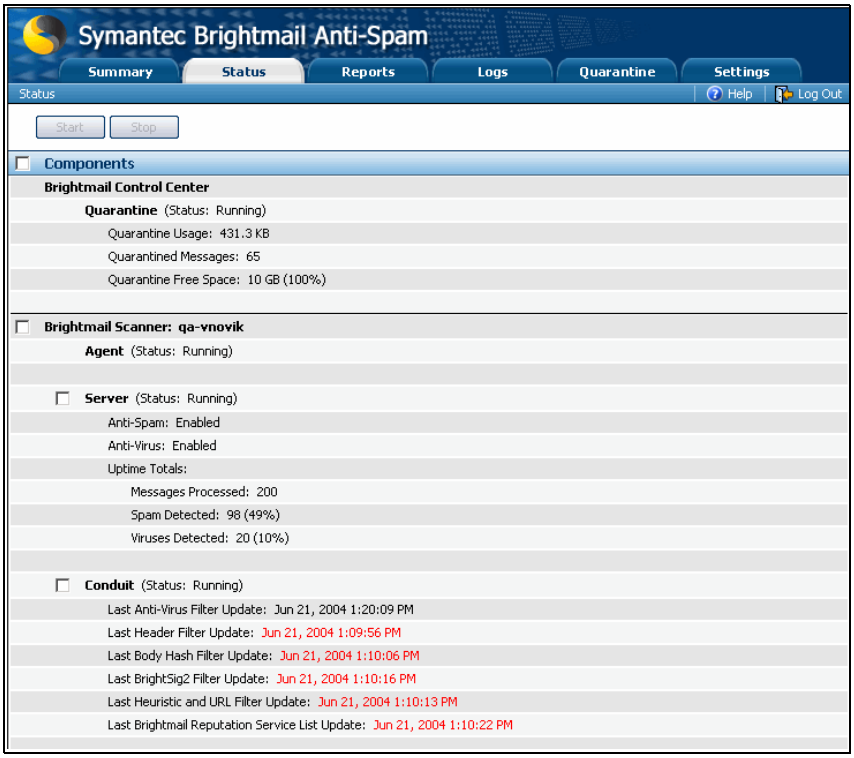
Table 3. Status Information for Brightmail Scanners and Components

Item	Component Description	Additional Status Information Provided
Harvester	Collects mail caught as spam by the Brightmail Server. Messages are forwarded to a previously configured email account or to the Quarantine.	N/A
Quarantine	Provides Web-based storage and management of quarantined mail.	Current quarantine disk space usage Number of messages in quarantine Disk free space
AntiVirus Cleaner	Provides antivirus filtering and cleaning.	Subscription Status. Antivirus filtering is available as a separate subscription. If you have not purchased a subscription for antivirus updates or if your subscription has expired, the AntiVirus Cleaner status area will indicate `Expired`. Contact your Symantec representative for instructions on renewing your subscription.

To view the status of scanners and components:

- In the Brightmail Control Center, click the **Status** tab.

  The Status page is displayed.



Starting and Stopping Symantec Brightmail AntiSpam

You can start and stop Brightmail Scanners and most components from the **Status** page. You can work with individual components on a specific Brightmail Scanner or you can start or stop all components on all Brightmail Scanners with one operation.

To start or stop Brightmail Scanners and components:

1. In the Brightmail Control Center, click the **Status** tab.
2. Select the Brightmail Scanner or component that you want to start or stop. To select all components on all Brightmail Scanners, select **Components**.
3. Do one of the following:
   - To stop a component or Brightmail Scanner that is currently running, click **Stop**.
   - To start a component or Brightmail Scanner that is currently stopped, click **Start**.

Managing Group Policies

This release of Symantec Brightmail AntiSpam introduces the concept of group policies: configurable message management options for an unlimited number of user groups which you define. Policies collect the antispam, antivirus, and content filtering verdicts and actions for a group.

This section includes the following topics:

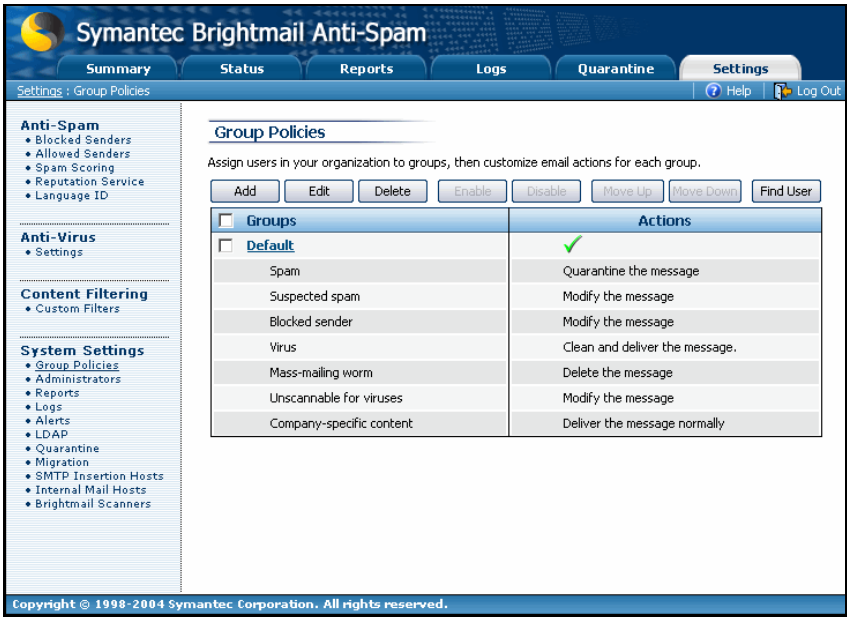
- Adding a Group Policy
- Managing Group Policies

Adding a Group Policy

You can specify groups of users based on email addresses or domain names. For each group, you can specify email filtering actions for different categories of email.

To create a new group policy:

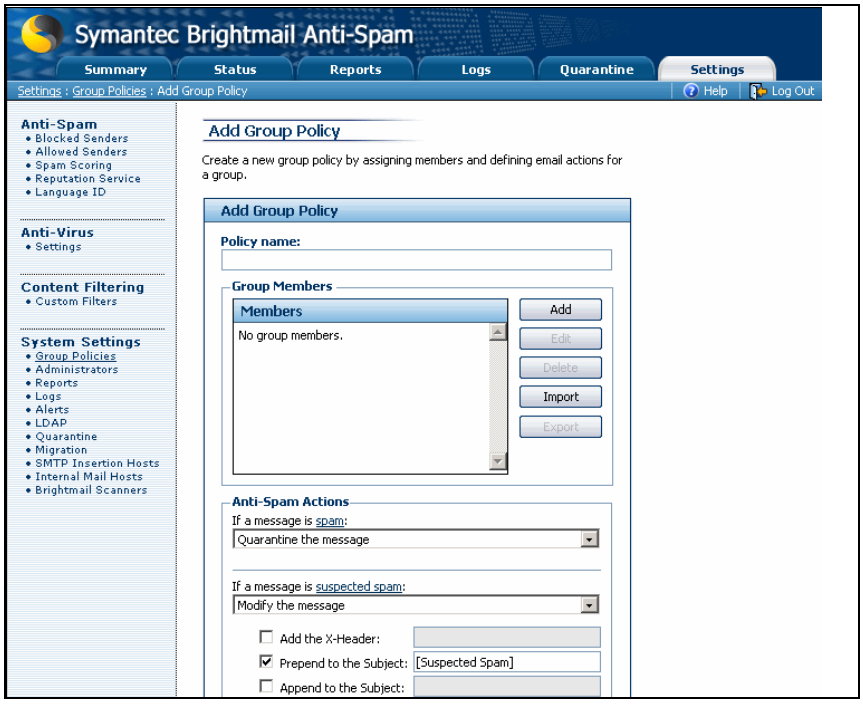
1. In the Brightmail Control Center, click the **Settings** tab.
2. In the left pane, click **Group Policies**.
   The Group Policies page is displayed.



For each group policy, this page maps email handling verdicts to associated actions. The **Default** group policy, which contains all users and all domains, appears last. Although you can add or modify actions for the **Default** group policy, you can neither add members to nor delete this group policy.

3 In the **Group Policies** page, click **Add**.

The Add Group Policies page is displayed.

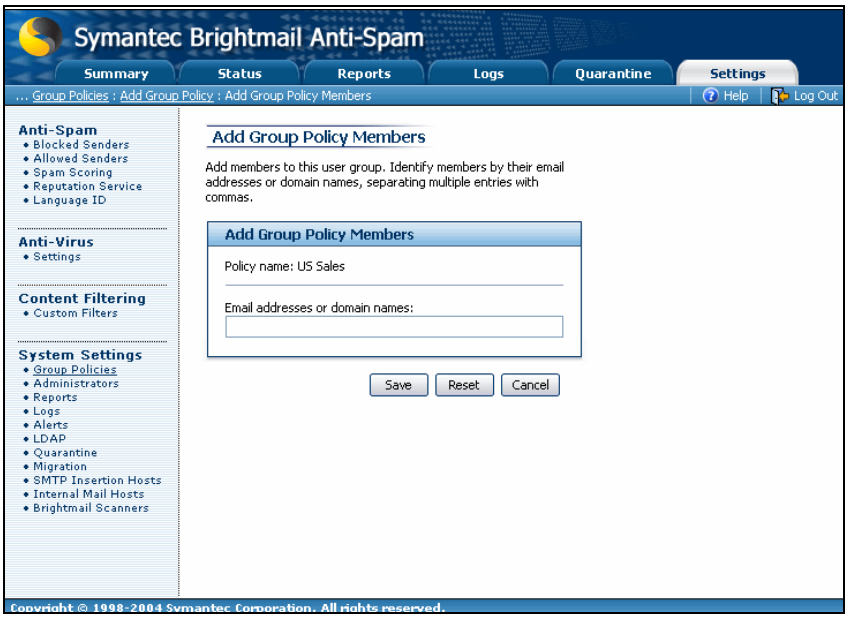


4 Enter a name in the **Group Policy Name** box.

To add a new member to this group policy:

1 Click **Add**.

The Add Group Policy Members page is displayed.



2 In the **Add Group Policy Members** page, type a valid value in the **Email addresses or domain names** box, separating multiple entries with commas. Use `*` to match zero or more characters and `?` to match a single character.

To add all recipients of a particular domain as members, type:

```
*@domain.com
```

3 Click **Save** to add the new member(s).

The **Add Group Policies Page** reappears.

4 Click **Save** to commit your changes to the group policy.

To delete a group policy member:

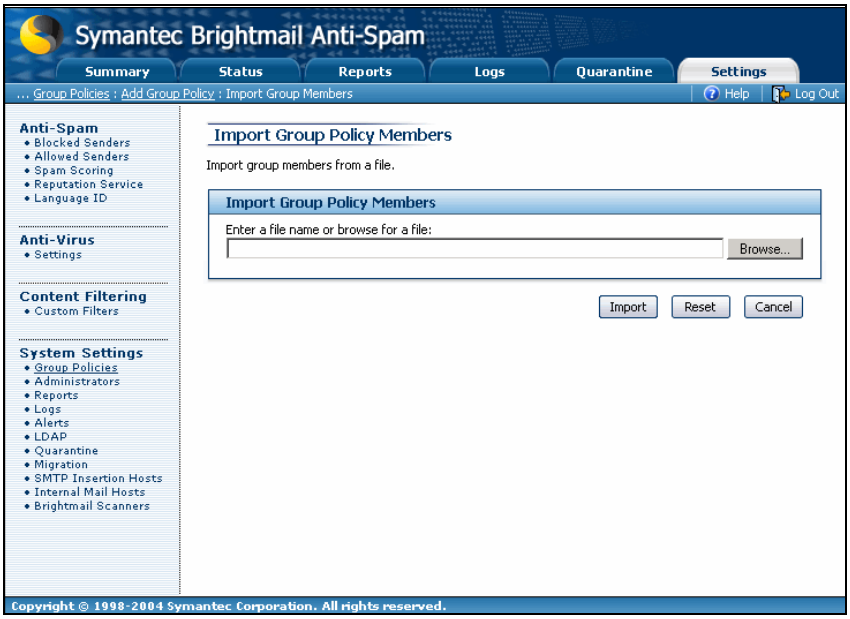
In the **Add Group Policy** page, select the check box next to a member's name, and then click **Delete**.

You can delete multiple members at the same time.

To import group policy members from a file:

1 In the **Add Group Policy** page, click **Import**.

The Import Group Policy Members page is displayed.



2 Enter the appropriate path and filename (or click **Browse** to locate the file on your hard disk), and then click **Import**.

The file should be a comma-delimited or newline-delimited plain text file. Below is a sample comma-delimited file:

```
ruth@example.com, rosa@example.com, ben*@example.com,
example.net, *.org
```

Below is a sample newline-delimited file:

```
ruth@example.com
rosa@example.com
ben*@example.com
example.net
*.org
```

In these examples:

- `ruth@example.com` and `rosa@example.com` match those exact email addresses.
- `ben*@example.com` matches `ben@example.com` and `benjamin@example.com`, etc.
- `example.net` matches all email addresses in `example.net`.
- `*.org` matches all email addresses in any domain ending with `.org`.

NOTE: *The maximum number of entries in the Group Members list for a group policy is 10,000. If you require more than 10,000 entries, contact your Symantec representative for instructions on how to configure MySQL and Tomcat to support more entries. This limitation refers to the number of entries in the Group Members list, not the number of users at your company.*

To export group policy members to a file:

1 In the **Add Group Policy** page, click **Export.**

2 Complete your operating system's save file dialog box as appropriate.

To define filtering actions for a new group policy:

Under each verdict, select a filtering action from the list.

The following table maps the available actions to the email handling verdicts:

Table 4. Email Handling Verdicts and Available Actions

Verdict	Available Actions
Spam, Suspected Spam, Blocked sender, Company-specific content	• Deliver the message normally • Delete the message • Deliver the message to the recipient's Spam folder[a] • Save the message to disk[b] • Forward the message • Quarantine the message • Modify the message
Mass-mailing worm	• Deliver the message normally • Delete the message
Virus	• Deliver the message normally • Delete the message • Clean and then deliver the message
Unscannable	• Deliver the message normally • Delete the message • Deliver the message to the recipient's Spam folder[a] • Save the message to disk[b] • Forward the message • Quarantine the message • Modify the message • Notify the recipient of unscannable reason

a) Lotus Domino requires Symantec Spam Folder Agent for Domino to folder spam. Exchange 2000 and 5.5 require the Spam Folder Agent. Exchange 2003 can folder spam with no additional software.

b) If you have a mix of UNIX and Windows Brightmail Scanners, do not use the `Save the message to disk` action.

NOTE: *Messages from senders in the Allowed Senders List are delivered directly to the recipient's inbox, bypassing any filtering (except antivirus filtering, if enabled). No other actions apply.*

Managing Group Policies

Brightmail AntiSpam's group policy management options let you do the following:

- Set group policy precedence, the order in which group policy membership is determined when policies are applied.
- Edit group policy membership and actions.
- Enable and disable group policies.
- Delete group policies.
- View group policy information for particular users.

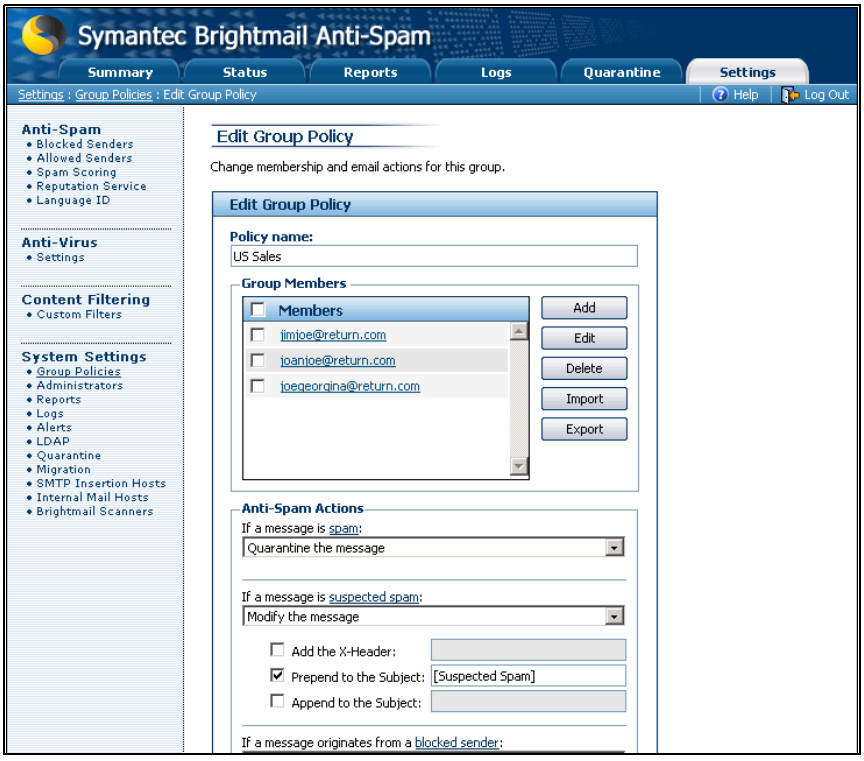
To set group policy precedence:

Select the check box next to a group policy, and then click **Move Up** or **Move Down** to change the order in which it is applied.

NOTE: *You cannot change the precedence of the **Default** group policy.*

To edit an existing group policy:

In the **Group Policy** page, select the check box next to a group policy, and then click **Edit**.



Add or delete members or change filtering actions for this group policy as you did when you created it. See "Adding a Group Policy," on page 33 for more information.

To enable a group policy:

Select the check box next to a group policy, and then click **Enable**.

To disable a group policy:

Select the check box next to a group policy, and then click **Disable**.

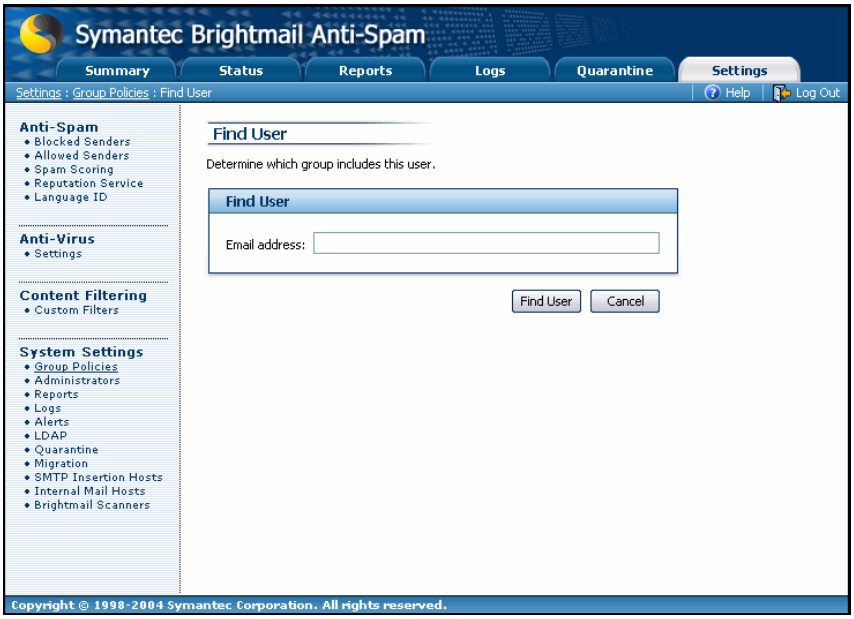
NOTE: *You cannot disable the **Default** group policy.*

To delete a group policy:

In the **Group Policies** page, select the check box next to a group policy, and then click **Delete**.

To view group policy information for a particular user or domain:

1 In the **Group Policies** page, click **Find User**.



2 Enter an email address or domain name, and then click **Find User**.

The page displays, listing the enabled group policy with the highest precedence to which the user or domain belongs.

Customizing Filtering at Your Site

Most customers find that the filters provided by Brightmail handle all their antispam needs. If you want to supplement Brightmail filtering, you can customize filtering at your site. For example, you can set up lists of allowed and blocked senders, adjust the criteria for suspected spam messages, create custom filters, and more.

The corresponding actions for the filters that you create and modify in this section are controlled by policies. To learn how to create policies, see "Managing Group Policies," on page 33.

This section includes the following topics:

- Specifying Allowed and Blocked Senders
- Adjusting Spam Scoring
- Enabling Language Identification
- Adjusting AntiVirus Settings
- Creating Custom Filters

Specifying Allowed and Blocked Senders

Filtering based on the source of the message, whether it's the sender's domain, email address or mail server IP connection, can be a powerful way to fine-tune filtering at your site.

NOTE: *The information in this section describes global blocked and allowed senders lists, which are applied at the server level for your organization. To give your users substantial control over spam management, you can deploy the* Symantec Plug-in for Outlook. *For more information on the* Symantec Plug-in for Outlook, *see the Symantec Brightmail AntiSpam Installation Guide.*

Symantec Brightmail AntiSpam lets you:

- **Define an Allowed Senders List –** Brightmail AntiSpam treats mail coming from an address or connection in the Allowed Senders List as legitimate mail. As a result, you ensure that such mail is delivered immediately to the inbox, bypassing any other filtering. The Allowed Senders List reduces the small risk that messages sent from trusted senders will be treated as spam or filtered in any way.

- **Define a Blocked Senders List –** Brightmail AntiSpam supports a number of actions for mail from a sender or connection on your Blocked Senders List. As with spam verdicts, you can use policies to configure a variety of actions to perform on such mail, including deletion, forwarding, and subject line modification.
- **Use the Brightmail Reputation Service –** By default, Brightmail AntiSpam is configured to use the Brightmail Reputation Service. Brightmail monitors hundreds of thousands of email sources to determine how much email sent from these addresses is legitimate and how much is spam. The service currently includes the following lists of IP addresses, which are continuously compiled, updated, and incorporated into the Brightmail AntiSpam filtering processes at your site:
  - **Open Proxy List** - IP addresses that are open proxies used by spammers.
  - **Safe List** - IP addresses from which virtually no outgoing email is spam.
  - **Suspect List** - IP addresses from which virtually all of the outgoing email is spam.

  No configuration is required for these lists. You can choose to disable the Open Proxy List or the Suspect List.
- **Incorporate lists managed by other parties –** Third parties compile and manage lists of desirable or undesirable IP addresses. These lists are queried using DNS lookups. When you configure Brightmail AntiSpam to use a third-party sender list, Brightmail AntiSpam checks whether the sending mail server is on the list. If so, Brightmail AntiSpam performs a configured action, based on the policies in place.

About Allowed and Blocked Senders Lists

Note the following about the Allowed Senders List and Blocked Senders List:

- **Overall filtering precedence –** In the process of determining an overall verdict for a message, Brightmail AntiSpam keeps track of the different filters that fire against a message. There are preset precedence rules that governs the ultimate verdict. For example, Brightmail AntiSpam gives a higher precedence to matches against the Allowed Senders and Blocked Senders Lists. In other words, matches against the Allowed Senders List and Blocked Senders List will “win” against conflicting filters created by Brightmail or custom filters created by you.
- **Precedence within the two lists –** If a message source falls into both the Allowed Senders List and the Blocked Senders List, the Allowed Senders List will have precedence and that message will be delivered to the inbox.

  Within the lists, IP addresses are generally more reliable for source filtering than email addresses, which are easily spoofed.

  In addition, lists that you create or (email-based and IP-based) will always have precedence over lists created by Brightmail. Note that list information from third party DNS blacklists that you specify does not have priority over Brightmail lists. In the event of a conflict between the Safe List (part of the Brightmail Reputation Service) and an entry from a DNS blacklist, the Brightmail-propagated list will win.The following list summarizes the precedence:

a. Allowed Senders List (IP addresses)
b. Allowed Senders List (third-party allowed senders services)
c. Blocked Senders List (IP addresses)
d. Allowed Senders List (email addresses)
e. Blocked Senders List (email addresses)
f. Safe List
g. Open Proxy List
h. Blocked Senders List (third-party blocked senders services)

- **Duplicate entries –** You cannot have the exact same entry in both the Blocked Senders List and the Allowed Senders List. If an entry already exists in one list, you will receive the message "`Duplicate sender - not added`" when you try to add it to the other list. The entry may not appear in the list you're working with. To move from one list to the other, delete it from the first and add it to the second. If you have two entries such as `a@b.com` and `*@b.com` in the two different lists, the precedence in the previous bullet wins.
- **Performance impact of third party DNS lists –** Incorporating third party lists adds additional steps to the filtering process. For example, in a DNS list scenario, for each incoming message, the IP address of the sending mail server is queried against the list, similar to a DNS query. If the sending mail server is on the list, the mail is flagged as spam. If your mail volume is sufficiently high, running incoming mail through a third party database could hamper performance because of the requisite DNS lookups. Brightmail recommends that you use the Brightmail Reputation Service instead of enabling third party lists.

Reasons to Use Allowed and Blocked Senders

The following table provides some examples of why you would employ lists of allowed or blocked senders. The table also lists an example of a pattern that you as the system administrator might use to match the sender:

Table 5. Use Cases for Lists of Allowed and Blocked Senders

Problem	Solution	Pattern Example
Mail from an end-user's colleague is occasionally flagged as spam.	Add colleague's email address to the Allowed Senders List.	`colleague@trustedco.com`
Desired newsletter from a mailing list is occasionally flagged as spam.	Add the domain name used by the newsletter to the Allowed Senders List.	`newsletter.com`

Table 5. Use Cases for Lists of Allowed and Blocked Senders (Continued)

Problem	Solution	Pattern Example
An individual is sending unwanted mail to people in your organization.	Add the specific email address to the Blocked Senders List.	`Joe.unwanted*@getmail.com`
Numerous people from a specific range of IP addresses are sending unsolicited mail to people in your organization.	After analyzing the received headers to determine the sender's network and IP address, add the IP address and net mask to the Blocked Senders List.	`218.187.133.191/ 255.255.0.0`

How Brightmail AntiSpam Identifies Senders and Connections

Supported Methods for Identifying Senders

You can use the following methods to identify senders for your Allowed Senders List and Blocked Senders List.

- **Specify sender addresses or domain names –** Brightmail AntiSpam checks the following characteristics of incoming mail against those in your lists:
  - — `MAIL FROM:` address in the SMTP envelope. Specify a pattern that matches the value for `localpart@domain` in the address. You can use wildcards in the pattern to match any portion of the address.
  - — `From:` address in the message headers. Specify a pattern that matches the value for `localpart@domain` in the From header. You can use wildcards in the pattern to match any portion of this value.
- **Specify IP connections –** Brightmail AntiSpam checks the IP address of the mail server initiating the connection to verify if it is on your Allowed Senders Lists or Blocked Senders Lists. Wildcards are not supported. Although you can use network masks to indicate a range of addresses, you cannot use subnet masks that define non-contiguous sets of IP addresses (e.g. `69.84.35.0/255.0.255.0`). Supported notations are:
  - — Single host: `128.113.213.4`
  - — IP address with subnet mask: `128.113.1.0/255.255.255.0`
- **Supply the lookup domain of a third party sender service –** Brightmail AntiSpam can check messages sources against third party DNS-based lists to which you subscribe.

Automatic Expansion of Subdomains

When evaluating domain name matches, Brightmail AntiSpam automatically expands the specified domain to include subdomains. For example, Brightmail AntiSpam expands `example.com` to include `biz.example.com` and, more generally, `*@*.example.com,` to ensure that any possible subdomains are allowed or blocked as appropriate.

Logical Connections and Internal Mail Servers: Non Gateway Deployments

When deployed at the gateway, Brightmail AntiSpam can reliably obtain the physical or peer IP connection for an incoming message and compare it to connections specified in the Allowed Senders List and Blocked Senders List. If deployed elsewhere in your network, for example, downstream from the gateway MTA, Brightmail AntiSpam works with the logical IP connection. Brightmail AntiSpam determines the logical connection by obtaining the address that was provided as an IP connection address when the message entered your network. Your network is based on the internal address ranges that you supply to Brightmail AntiSpam when setting up your Brightmail Scanners. This is why it is important that you accurately identify all the internal mail hosts in your network. For more information, see "Specifying Internal Mail Hosts," on page 26.

Adding Senders to Your Blocked Senders List

To prevent undesired messages from being delivered to inboxes, you can add specific email addresses, domains, and connections to your Blocked Senders List.

To add email addresses, domains, and third-party lists to your Blocked Senders List:

1. In the Brightmail Control Center, click the **Settings** tab.
2. In the left pane, under **AntiSpam**, click **Blocked Senders**.
3. Click **Add**.
4. In the **Add Blocked Senders** page, do any or all of the following:

Table 6. Sample Values for Blocked Senders Lists

For this box…	Supply the Following Information	
Blocked email addresses or domain names	Identify a sender address. If the address or domain you specify matches an incoming message's SMTP envelope `FROM` address, header `From` address, or both, the message is considered to be from a blocked sender. Brightmail AntiSpam automatically filters the subdomains on the specified domain. The message will be handled based on the policies set in place. **Acceptable characters:** All alphanumerics and special characters, except the plus sign (+). **Wildcards:** Use * to match zero or more characters and ? to match a single character.	
	Example	**Matches**
	`example.com`	`chang@example.com, marta@example.com, foo@bar.example.com`
	`malcolm@example.net`	`malcolm@example.net`
	`sara*@example.org`	`sara@example.org, sarahjane@example.org`
	`jo??@example.org`	`john@example.org, josh@example.org`

Table 6. Sample Values for Blocked Senders Lists

For this box…	Supply the Following Information
Blocked IP addresses	Identify the numerical IP address for hosts from which to block connections. You can use subnet masks. You cannot use subnet masks that define non-contiguous sets of IP addresses (e.g. `67.84.37.0/255.0.255.0`) **Wildcards:** Not permitted. **Example:** `192.0.2.0`
Third Party Blocked Senders Services	Specify a third party DNS blacklist to which you subscribe. **Wildcards:** Not permitted. **Example:** `blacklist.example.org`

5 Click **Save**.

Adding Senders to Your Allowed Senders List

To ensure that messages from specific email addresses, domains, and connections are not treated as spam, you can add them to your Allowed Senders List.

To add email addresses, domains, and third-party lists to your Allowed Senders List:

1 In the Brightmail Control Center, click the **Settings** tab.

2 In the left pane, under **AntiSpam**, click **Allowed Senders**.

3 Click **Add**.

4 In the **Add Allowed Senders** page, do any or all of the following:

Table 7. Example Values for Allowed Senders List

For this box…	Supply the Following Information	
Allowed email addresses or domain names	Identify a sender address. If the address or domain you specify matches an incoming message's SMTP envelope `FROM` address, header `From` address, or both, the message is considered to be from a trusted sender and is delivered normally. Brightmail AntiSpam automatically filters the subdomains on the specified domain. **Acceptable characters:** All alphanumerics and special characters, except the plus sign (+). **Wildcards:** Use * to match zero or more characters and ? to match a single character.	
	Example	**Matches**
	`example.com`	`chang@example.com, marta@example.com, foo@bar.example.com`
	`malcolm@example.net`	`malcolm@example.net`
	`sara*@example.org`	`sara@example.org, sarahjane@example.org`
	`jo??@example.org`	`john@example.org, josh@example.org`

Table 7. Example Values for Allowed Senders List (Continued)

For this box…	Supply the Following Information
Allowed IP addresses	Identify the numerical IP address for hosts from which to allow connections. You can use subnet masks. You cannot use subnet masks that define non-contiguous sets of IP addresses (e.g. `64.85.36.0/255.0.255.0`) **Wildcards:** Not permitted. **Example:** `192.0.2.0`
Third Party Allowed Senders Services	Specify a third party DNS whitelist to which you subscribe. **Wildcards:** Not permitted. **Example:** `whitelist.example.org`

5 Click **Save**.

The Allowed Senders List updates to reflect the sender information you specified.

Deleting Senders from Lists

To delete senders from your Blocked Senders List or Allowed Senders List:

1 In the Brightmail Control Center, click the **Settings** tab.

2 In the left pane, under **AntiSpam**, click **Blocked Senders** or **Allowed Senders**, depending on the list that you want to work with.

3 In the list of senders, click the check box next to the sender that you want to remove from your list, and then click **Delete**.

Editing Senders

To edit information for senders in your Blocked Senders List or Allowed Senders List:

1 In the Brightmail Control Center, click the **Settings** tab.

2 In the left pane, under **AntiSpam**, click **Blocked Senders** or **Allowed Senders**, depending on the list that you want to work with.

3 In the list of senders, click the check box next to the sender whose information you want to modify, and then click **Edit**.

You can also click an underlined sender name to automatically jump to the corresponding edit page.

4 Make any changes, and then click **Save**.

Enabling or Disabling Senders

When you add a new sender to your Blocked Senders List or Allowed Senders List, Brightmail AntiSpam automatically enables the filter and puts it to use when evaluating incoming messages. You may need to periodically disable and then re-enable senders from

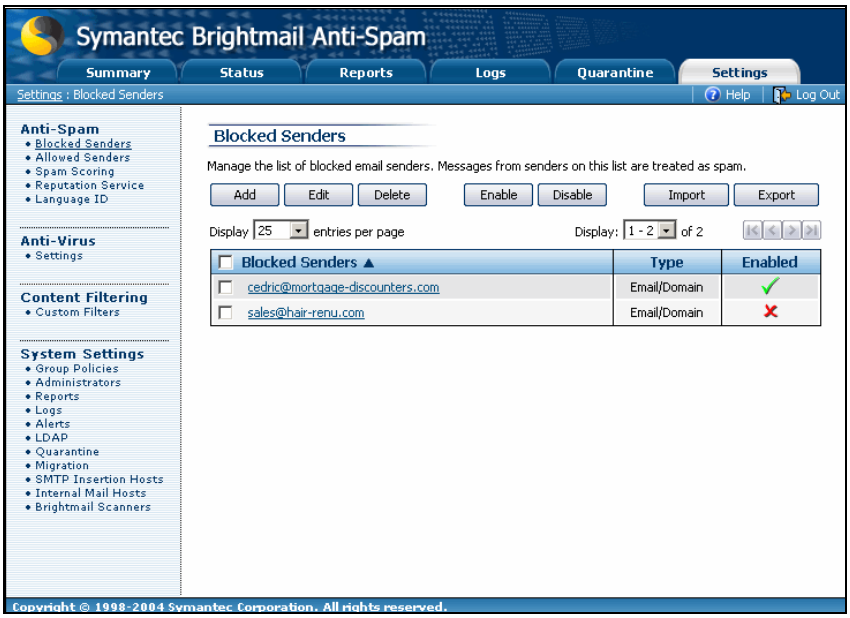
your list for troubleshooting or testing purposes or if your list is not up to date. Brightmail AntiSpam will treat mail from a sender that you've disabled just as it would any other message.

To enable or disable senders from your lists:

1 In the Brightmail Control Center, click the **Settings** tab.

2 In the left pane, under **AntiSpam**, click **Blocked Senders** or **Allowed Senders**.

The page you selected is displayed.



A red x (✗) in the Enabled column indicates that the entry is currently disabled. A green check mark (✓) in the Enabled column indicates that the entry is currently enabled.

3 In the list of senders, do one of the following:

— To enable a sender entry that is currently disabled, click the check box adjacent the sender information, and then click **Enable**.

— To disable a sender entry that is currently enabled, click the check box adjacent the sender information, and then click **Disable**.

Importing Sender Information

If you have many senders and addresses to add to your Blocked Senders List or Allowed Senders List, it is often easier to place the sender information in a text file and then import the file.

To add sender information, patterns and DNS zones, you need to modify a text file (`allowedblockedlist.txt`) that is provided with your Brightmail AntiSpam software. This section describes how to edit that file.

The file is line-oriented and uses a format similar to LDIF. It has the following restrictions and characteristics:

- The file must have the required LDIF header that is included upon installation
- Each line contains exactly one attribute, along with a corresponding pattern
- Empty lines or white spaces are not allowed
- Lines beginning with # are ignored
- Entries terminating with the colon-dash pattern (:-) are disabled; entries terminating with the colon-plus pattern (:+) are enabled;

To populate the list, specify an attribute, which is followed by a pattern. In the following example, a list of attributes and patterns follows the LDIF header.

```
## Permit List
#
dn: cn=mailwall@brightmail.com, ou=bmi
objectclass: top
objectclass: bmiBlackWhiteList
AC: 65.86.37.45/255.255.255.0
AS: grandma@aol.com
RC: 20.45.32.78/255.255.255.255
RS: spammer@aol.com
BL: spl.spamhaus.org
# Example notations for disabled and enabled entries follow
RS: rejectedspammer@aol.com:-
RS: rejectedspammer2@aol.com:+
```

The attributes and the syntax for the values are as follows:

Table 8. Syntax for Preparing Importable List for Allowed and Blocked Senders

Attribute	Meaning	Acceptable Values	Example Values
AC:	Allowed connection or network.	Numerical IP address and network mask of host to allow or block using the format a.b.c.d/e.f.g.h **Wildcards:** Not permitted	Single IP address: AC:76.86.37.45/255.255.255.255 AC:76.86.37.45 Class C network: RC: 76.87.37.0/255.255.255.0
RC:	Rejected or blocked connection/network		
AS:	Allowed sender	All alphanumerics and special characters, except the plus sign (+). **Wildcards:** Use * to match many characters and ? to match a single character.	Single sender address: RS: spammer@aol.org Fixed size noisy address: RS: john?????@domain.com
RS:	Rejected or blocked sender		
BL:	Third party blocked sender server	Numerical IP address or canonical name of a third party whitelist or blacklist service. **Wildcards:** Not permitted	BL: spl.spamhaus.org
WL:	Third party allowed sender service		WL: senderbase.org

To import sender information from an `allowedblockedlist.txt` file:

1. In the Brightmail Control Center, click the **Settings** tab.
2. In the left pane, under **AntiSpam**, click **Blocked Senders** or **Allowed Senders**.
3. Click **Import**.
4. In the **Choose File** dialog box, specify the location of the your text file with the sender information, and then click **Open**. Ensure that the sender information is formatted as described earlier in this section.
5. Click **Import**.

   Brightmail AntiSpam merges data from the imported list with the existing sender information.

Exporting Sender Information

You can easily export to a single file all the information in your Allowed Senders List and Blocked Senders List.

To export sender information from your Blocked Senders List or Allowed Senders List:

1. In the Brightmail Control Center, click the **Settings** tab.
2. In the left pane, under **AntiSpam**, click **Blocked Senders** or **Allowed Senders**.

NOTE: *You do not need to select check boxes next to individual sender names. The Export feature exports the entire list.*

3. Click **Export**.

   Your browser will prompt you to open the file from its current location or save it to disk.

Customizing the Brightmail Reputation Service

The Brightmail Reputation Service is a service managed by Brightmail that continuously compiles and updates the following lists of IP addresses:

- **Open Proxy List –** IP addresses that are open proxies used by spammers.
- **Safe List –** IP addresses from which virtually no outgoing email is spam.
- **Suspect List –** IP addresses from which virtually all of the outgoing email is spam.

Brightmail monitors hundreds of thousands of email sources to determine how much email sent from these addresses is legitimate and how much is spam. Email from given email sources can then be blocked or allowed based on the source's reputation value as determined by Brightmail.

By default, Brightmail AntiSpam is configured to incorporate the source information from all three lists in the Brightmail Reputation Service. If you want to specify the lists to use, follow the procedures in this section.

To select lists in the Brightmail Reputation Service:

1 In the Brightmail Control Center, click the **Settings** tab.

2 In the left pane, under **AntiSpam**, click **Reputation Service**.

The Brightmail Reputation Service page is displayed.

3 Under **Brightmail Reputation Service Lists**, clear the check boxes for the lists that you do not want to use.

You cannot disable the **Suspect List**.

4 Click **Save**.

Adjusting Spam Scoring

When evaluating whether messages are spam, Brightmail AntiSpam calculates a spam score from 1 to 100 for each message, based on techniques such as pattern matching and heuristic analysis. If an email scores in the range of 90 to 100 after being filtered by Brightmail AntiSpam, it is defined as spam.

For more aggressive filtering, you can optionally define a discrete range of scores below 90 and above 25. The messages that score within this range will be considered *suspected spam*. Unlike spam, which is determined by Brightmail and not subject to adjustment by administrators, suspected spam is a separate category that you set on the Spam Scoring page. Using policies, you can specify different actions for messages identified as suspected spam and messages identified as spam by Brightmail.

For example, assume that you have configured your suspected spam scoring range to encompass scores from 80 and 89. If an incoming message receives a spam score of 89, Brightmail AntiSpam will consider this message to be suspected spam, and will apply the

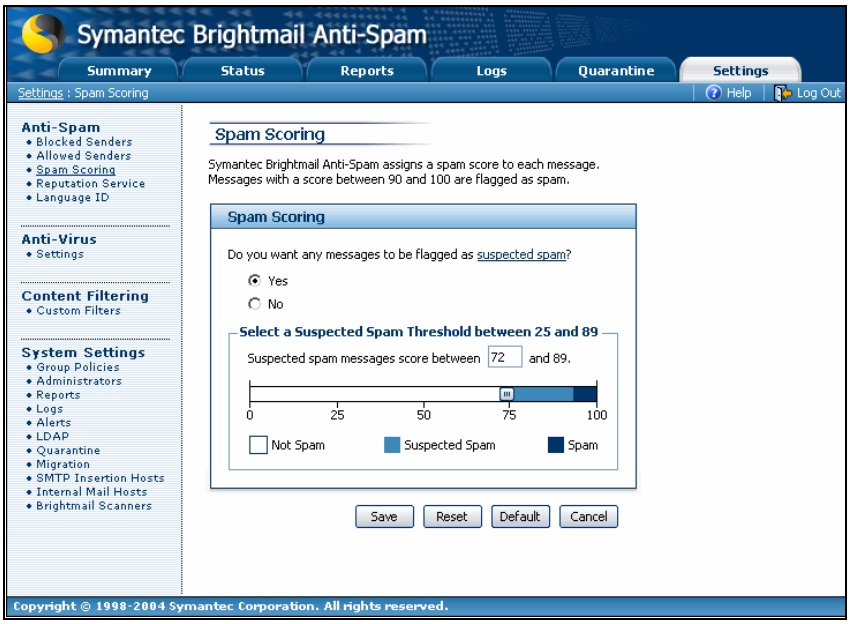
action you have in place for suspected spam messages, such as **Modify the Message** (tagging the subject line). Messages that score 90 or above will not be affected by the suspected spam scoring setting, and will be subject to the action you have in place for spam messages, such as **Quarantine the Message**.

NOTE: *Brightmail recommends that you not adjust the spam threshold until you have some visibility into the filtering patterns at your site. Then, gradually move the threshold setting down 1 to 5 points a week until the number of false positives is at the highest level acceptable to you. You can test the effects of spam scoring by setting up a designated mailbox or user to receive false positive notifications to monitor the effects of changing the spam score threshold.*

To adjust the spam score for suspected spam:

1. In the Brightmail Control Center, click the **Settings** tab.
2. In the left pane, under **AntiSpam**, click **Spam Scoring**.

   The Spam Scoring page is displayed.



3. Under **Do you want any messages to be flagged as suspected spam**, click **Yes**.
4. Click and drag the slider to increase or decrease the lower bound of suspected spam range. You can also type a value in the box.
5. Click **Save**.

Enabling Language Identification

NOTE: *You can use the Language Identification feature only if you are using the* Symantec Plug-in for Outlook *software on user desktops. Disregard this section if you are not using this software.*

Brightmail AntiSpam can determine the language in which a filtered message is written. By default, Brightmail AntiSpam treats all languages equally. When used together with the optional Symantec Plug-in for Outlook software deployed on desktops, language identification can help increase filtering effectiveness. Within the Symantec Plug-in for Outlook software, users can specify that all messages identified as written in certain languages be treated as spam. If an incoming message is identified in a language that is not one of the allowed languages, Brightmail AntiSpam will automatically treat that message as spam.

To enable language identification:

1. In the Brightmail Control Center, click the **Settings** tab.
2. In the left pane, under **AntiSpam**, click **Language ID**.

   The Language Identification page is displayed.

3. Under **Do you want to enable Language Identification**, click **Yes**.

   Only select this option if you are deploying the Symantec Plug-in for Outlook and using the Plug-in's language feature.
4. Click **Save**.

Adjusting AntiVirus Settings

NOTE: *If your antivirus subscription has expired, an expiration message will appear next to the AntiVirus Cleaner component on the Status page. If your subscription lapses, virus filtering will cease. Contact your Symantec representative for instructions on purchasing or renewing virus filtering.*

When configured for antivirus filtering, Brightmail Scanners detect viruses from email as it enters your email system. When one or more viruses are detected, the antivirus policies you have set up go into effect. For example, you can instruct the Brightmail Scanner to:

- Deliver the message normally
- Delete the message
- Clean the message with the AntiVirus Cleaner and then redeliver the message using an SMTP process

You can also set policies for mass-mailing worms and potential virus messages that cannot be processed by Brightmail Scanner (unscannable messages).

After processing messages, the AntiVirus Cleaner creates a configurable advisory text message. This message informs the user that the infected attachment has been cleaned, deleted, or delivered without cleaning. The Cleaner inserts the original message, if delivered, as an attachment to the advisory message. The Cleaner also places a special identifying line in the message header so that the message is not filtered again for viruses. See Appendix B, “Editing Virus Notification Messages,” on page 139 for details on the text the Cleaner adds in each case and instructions on how to customize the text.

Available Settings

The available configuration settings for antivirus filtering include the following:

- **Enabling and disabling –** For testing or troubleshooting purposes, you may need to temporarily disable and then re-enable antivirus filtering.
- **Setting the heuristic level –** The heuristic level determines the way in which viruses are flagged. A higher heuristic level will cause Brightmail AntiVirus to be more aggressive in flagging viruses.
- **Dealing with potential zip bombs and large files –** When Brightmail AntiSpam extracts and processes certain zip files and other types of compressed files, these files can expand to the point where they deplete system memory. Such files are often referred to as “zip bombs.” Brightmail AntiSpam can handle such situations by automatically sidelining large attachments and cleaning them. There is a presumption that such a file can be a “zip bomb” and should not be allowed to over-use the

resources of the Brightmail AntiSpam. The file is sidelined for cleaning only because of its size, not because of any indication that it contains a virus.

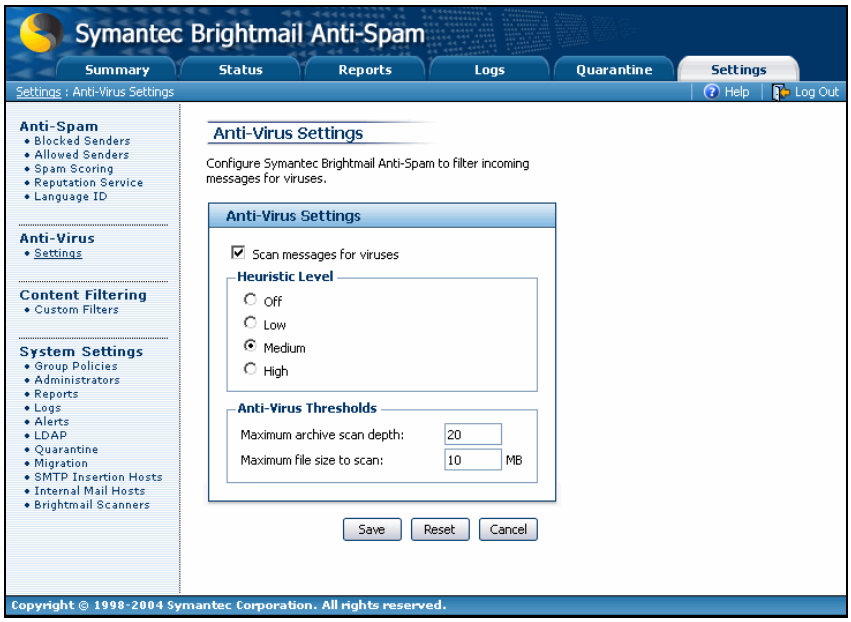
NOTE: *In some cases, where the size of the file or the number of nested levels exceeds the resources available for processing, the file cannot be cleaned. If it cannot be cleaned it will be deleted. If it cannot be deleted, an appropriate advisory message is included, notifying the recipient that antivirus cleaning was not possible.*

You can specify this size threshold, as well as the maximum extraction level that Brightmail AntiSpam will process in memory. If the configured limits are reached, Brightmail AntiSpam will automatically perform the action designated for the "unscannable" category in the Group Policies settings.

To configure antivirus filtering:

1. In the Brightmail Control Center, click the **Settings** tab.
2. In the left pane, under **AntiVirus**, click **Settings**.

   The Anti Virus Settings page is displayed.



3. To enable antivirus filtering, click **Scan messages for viruses**.
4. Under **Heuristic Level**, select the level for the antivirus scanning engine.
5. In the **Maximum archive scan depth** box, specify a depth level for recursively compressed zipped archive files.

   After this point, Brightmail AntiSpam will treat the message as unscannable, stop processing, and apply the action you have in place for the unscannable category.

Do not set this value too high or you could be vulnerable to a zip bomb, in which huge amounts of data are zipped into very small files. Do not set this value too low, or nested sets of replies and forwards on legitimate messages could trigger the threshold.

6 In the **Maximum file size to scan** box, specify a maximum attachment size in megabytes. After this point, Brightmail AntiSpam will treat the message as "unscannable," stop processing, and apply the action you have in place for the unscannable category.

Do not set this value too high or you could be vulnerable to a zip bomb.

7 Click **Save**.

To verify that the antivirus filtering is enabled, click the **Status** tab and ensure the **AntiVirus Cleaner** component is enabled and running.

Creating Custom Filters

You can create custom filters based on key words and phrases found in specific areas of a message. By writing filters at the server level, you can supplement Brightmail AntiSpam. Based on policies you set up, you can perform a wide variety of actions on messages that match against your custom filters.

Custom filters can be used to:

- Eliminate spamming viruses by blocking messages with specific body content, or specific file attachment types or filenames.
- Control message volume and preserve disk space by filtering out oversized messages.
- Block email from marketing lists that generate user complaints or use up excessive bandwidth.
- Block messages containing certain text in their headers or bodies.

Actions specified for custom filter matches will not override actions resulting from matches in your Blocked Senders List or Allowed Senders List or from matches against antispam filters created by Brightmail. In other words, if a message's sender matches an entry in your Blocked Senders List or Allowed Senders List or if a message is determined to be spam by Brightmail, custom filters will have no effect on the message.

Using the Custom Filters Editor

The Custom Filters Editor provides a way to create custom filters without programming them in the Sieve language.

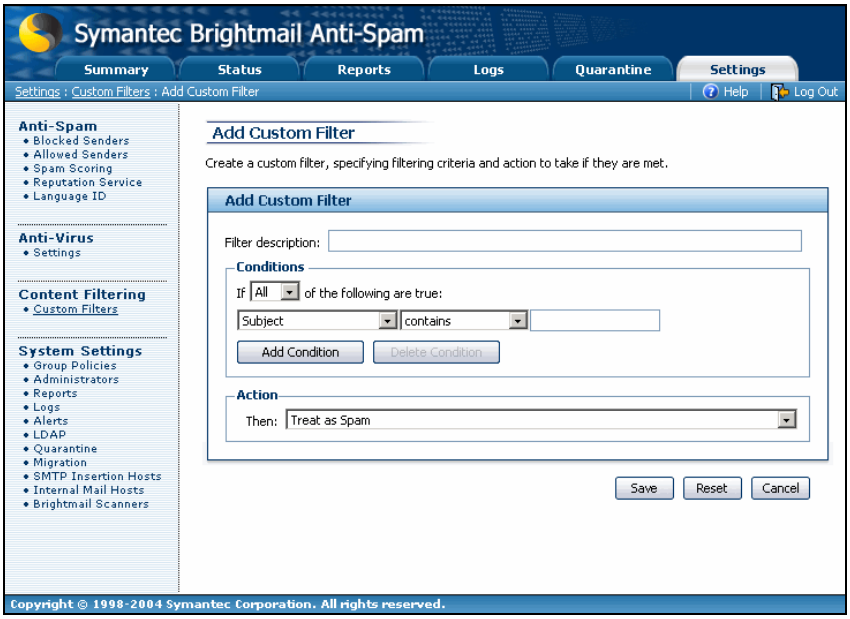
NOTE: *If you would rather work with a hand-coded Sieve file, see* "Importing a Custom Filters File," on page 64. *Make sure you are familiar with Brightmail's implementation for Sieve, described in* "Creating Filters by Coding in Sieve," on page 129.

To create custom filters:

1 In the Brightmail Control Center, click the **Settings** tab.

2 In the left pane, under **Content Filtering**, click **Custom Filters**.
The Custom Filters page is displayed.

3 Click **Add**.
The Add Custom Filter page is displayed.



4 Describe this filter in the **Filter Description** box. The description will also be displayed on the main Custom Filters Editor window.

5 Choose **All** or **Any** to determine if all or any one of the conditions you set in this filter must be met for the filter to trigger.

This setting has no effect for filters with only one condition.

6 Each row in the filter is called a condition. For each condition, choose the message component and value to test against. See Table 9, "Filter Components" and Table 10, "Filter Tests" for a description of the choices.

7 Click **Add Condition** to add a new condition.

To remove the bottommost condition, click **Delete Condition**.

8 In the **Action** section, use the **Then** list to choose one of following categories for messages when the conditions in the filter are met:

- Treat as Spam
- Treat as Suspected Spam
- Treat as Allowed Sender
- Treat as Blocked Sender
- Treat as Mass Mailing Worm
- Treat as Unscannable for Viruses
- Treat as Company-Specific Content
- Deliver the Message Normally

You can use group policies to control what happens to messages that fall into these categories. See "Managing Group Policies," on page 33 for more information.

9 Click **Save**. The list of Custom Filters updates to include the filter you created.

Creating Conditions in Custom Filters

Table 9, "Filter Components" describes the rule components available in the first in Step 6 above.

Table 9. Filter Components

Component Name	Test Against	Examples

`Envelope From Address`	From address in the message envelope. The envelope information is not usually visible in mail reading programs like Outlook.	`jane`
		`example.com`
		`jane@example.com`

`Envelope To Address`	To address in the message envelope. The envelope information is not usually visible in mail reading programs like Outlook.	`jane`
		`example.com`
		`jane@example.com`

`Envelope Helo Domain`	Sending domain listed in the `HELO`/`EHLO` SMTP command.The envelope information is not usually visible in mail reading programs like Outlook.	`com`
		`example`
		`example.com`

Table 9. Filter Components (Continued)

Component Name	Test Against	Examples
`Peer IP`	IP address of the SMTP client that has contacted the local MTA. Type the peer IP in one of these formats: • Single host: `128.113.213.4` • Netmask Source-IP: `128.113.1.0/255.255.255.0` The envelope information is not usually visible in mail reading programs like Outlook.	See the examples at left

`From Address`	From message header.	`jane`
		`example.com`
		`jane@example.com`

`To Address`	To message header.	`jane`
		`example.com`
		`jane@example.com`

`Cc Address`	Cc (carbon copy) message header.	`jane`
		`example.com`
		`jane@example.com`

`Bcc Address`	Bcc (blind carbon copy) message header.	`jane`
		`example.com`
		`jane@example.com`

`Recipient`	To, Cc, and Bcc message header.	`jane`
		`example.com`
		`jane@example.com`

`Correspondent`	From, To, Cc, and Bcc message header.	`jane`
		`example.com`
		`jane@example.com`

`Sender`	Sender message header.	`jane`
		`example.com`
		`jane@example.com`

`Subject`	Subject message header.	`$100 F R E E, Please Play Now!`

`Header Field`	Message header specified in the accompanying text field. A header is case-insensitive. Don't type the trailing colon in a header.	`Reply-To`
		`reply-to`
		`Message-ID`

`MIME Header`	Message header or MIME header specified in the accompanying text field. A header is case-insensitive. Don't type the trailing colon in a header.	`Reply-To`
		`reply-to`
		`Content-Type`
		`Content-Disposition`

Table 9. Filter Components (Continued)

Component Name	Test Against	Examples
`Message Body`	Contents of the message body. This component test is the most processing intensive, so you may want to add it as the last condition in a filter to optimize the filter.	`You already may have won`

`Size`	Size of the message in bytes, kilobytes, or megabytes, including the header and body.	`2`
		`200`
		`2000`

Table 10, "Filter Tests" describes the filter tests available in the second drop-down list in Step 6 above.

Table 10. Filter Tests

Test Type	Characters * and ? Act As Wildcards?	Description
`Is`	`No`	Exact match for the supplied text
`Contains`	`No`	Tests for the supplied text within the component specified. This is sometimes called a substring test.
`Starts with`	`No`	Equivalent to `text*` wildcard test using `Matches`.
`Ends With`	`No`	Equivalent to `*text` wildcard test using `Matches`.
`Matches`	`Yes`	Match for the string using wildcards, if supplied.
`Exists`	`No`	Tests for the presence of the message header in the drop-down list or typed in the text box.
Notes: All text tests are case-insensitive. There are also negative Test Types. Some tests are not available for some components.		

Using Wildcards With the Matches and Does not Match Tests

If you specify the Matches or Does not Match test for a component, you can use the `*` and `?` wildcard characters as described in Table 11, "Using Wildcards in Matches and Does not Match Tests". To match either `*` or `?` you have to precede each with `\` as shown in the table. It is valid to use multiple instances of `*`, `?`, `\*`, and `\?` in combination with normal characters in the same search term.

Table 11. Using Wildcards in Matches and Does not Match Tests

Character(s)	Description	Example	Sample Matches
*	Match zero or more characters	`sara*`	`sara`, `sarah`, `sarahjane`, `saraabc%123`
		`s*m*`	`sam`, `simone`, `sm`, `s321m$xyz`

Table 11. Using Wildcards in Matches and Does not Match Tests (Continued)

Character(s)	Description	Example	Sample Matches
?	Match any one character	j?n	jen, jon, j2n, j$n
		jo??	john, josh, jo4#
*	Match the asterisk character	b**	b**
\?	Match the question mark character	now\?	now?

Guidelines for Creating Conditions

Keep these suggestions and requirements in mind as you create the conditions that make up a filter.

- There is no limit to the number of conditions per filter.
- It's possible to create custom filters that block or allow email based upon the sender information, but usually it's best to use the Allowed Senders List and Blocked Senders List. However, it's appropriate to create custom filters if you need to block or keep email based on a combination of the sender and other criteria, such as the subject or recipient.
- All tests for words and phrases are case-insensitive, meaning that lowercase letters in your conditions match lower- and uppercase letters in messages, and uppercase letters in your conditions match lower- and uppercase letters in messages. For example, if you tested that the subject contains "inkjet", then "inkjet", "Inkjet", and "INKJET" in a message subject would match. If you instead tested for "INKJET" in the subject, then "inkjet", "Inkjet", and "INKJET" would still match. This applies to all test types and all filter components.
- Multiple white spaces in an email header or body are treated as a single space character. For example, if you tested that the subject contains "inkjet cartridge", then "inkjet cartridge" and "inkjet cartridge" in a message subject would match. If you instead tested for "inkjet cartridge" in the subject, then "inkjet cartridge" and "inkjet cartridge" would still match. This applies to all test types and all filter components. A message subject containing "i n k j e t c a r t r i d g e" would not match a test for "inkjet cartridge" or "inkjet cartridge".
- The order of conditions in a filter does not matter as far as whether a filter matches a message. However, if a filter has Message Body tests, you can optimize the filter by positioning them as the final conditions in a filter.
- Spammers usually "spoof" or forge some of the visible messages headers and the usually invisible envelope information. Sometimes they forge header information using the actual email addresses or domains of innocent people or companies. So use care when creating filters against spam you've received.

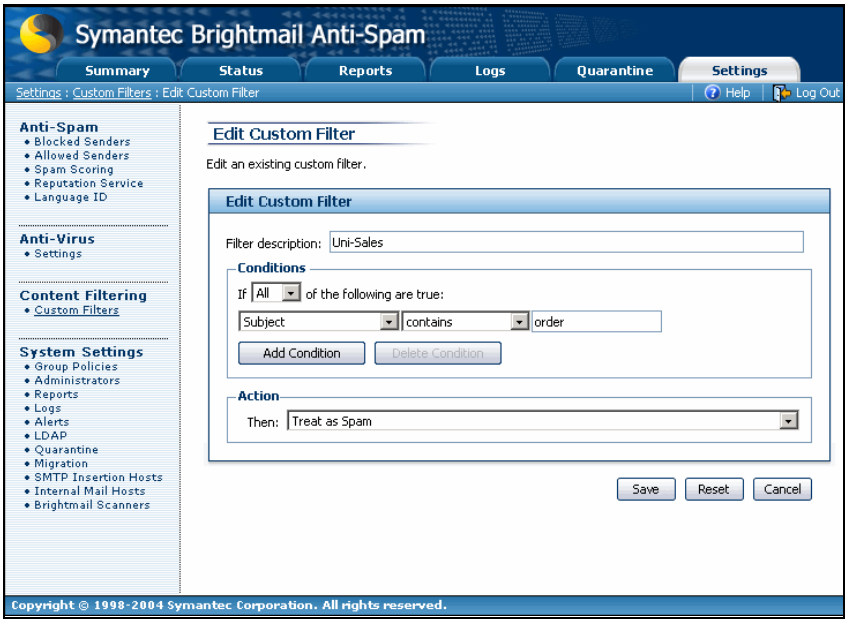
Editing Filters

To edit a filter in the list:

1. In the Brightmail Control Center, click the **Settings** tab.
2. In the left pane, under **Content Filtering**, click **Custom Filters**.
3. In the list of filters, click the check box next to the filter you want to modify, and then click **Edit**.

   You can also click an underlined filter description to display the corresponding edit page.

   The Edit Custom Filter page is displayed.



4. Change the filter as needed:
   - To change the **Filter description**, edit the existing text.
   - To change whether all or any one of the conditions you set in this filter must be met for the action, choose **All** or **Any**.
   - To change a condition, modify the list and boxes as appropriate. Each row in the filter is called a condition.
   - To add a condition, click **Add Condition**.
   - To delete a condition, click **Delete Condition**. You can only delete the bottommost condition.
   - To change the action of matching messages, choose an item from the list.
5. Click **Save** to accept your changes.

Deleting Filters

You can delete a filter that you have created if it is not meeting your needs. If you need to temporarily disable a filter without permanently deleting it, see "Enabling and Disabling Filters," on page 64.

To delete a filter from the list:

1. In the Brightmail Control Center, click the **Settings** tab.
2. In the left pane, under **Content Filtering**, click **Custom Filters**.
3. Click the check box next to the filter you want to delete.
4. Click **Delete**.

   The filter is deleted immediately.

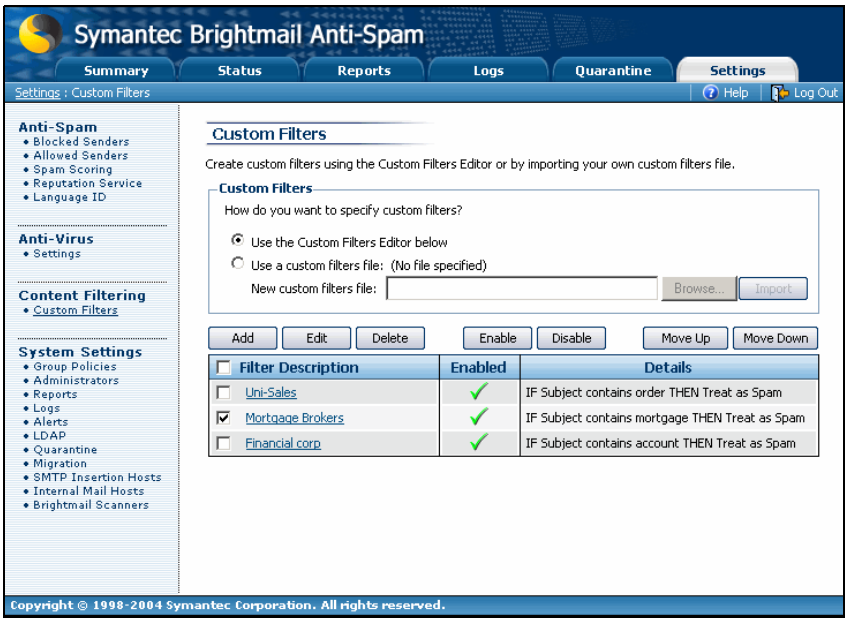
Determining Filter Order

Filters are evaluated in the order displayed on the list. If a message triggers more than one filter, the action of the first filter triggered will be performed on the message. To change the order of the filters in the list, follow the procedure in this section. It's best to position filters that you think will match more often earlier in the list.

To change the order by which filters are checked:

1. In the Brightmail Control Center, click the **Settings** tab.
2. In the left pane, under **Content Filtering**, click **Custom Filters**.

   The Custom Filters page is displayed.



3. Select the Custom Filter you want to move.

4 Click **Move Up** or **Move Down** to move the selected filter up or down in the list of filters.

Enabling and Disabling Filters

After you create custom filters, they are automatically enabled and put to use. For testing or other administrative purposes, you may need to enable or disable one or more filters without having to delete them. By disabling filters, filters become inactive but are displayed in the main Custom Filter list.

To enable or disable filters in the Custom Filters list:

1 In the Brightmail Control Center, click the **Settings** tab.

2 In the left pane, under **Content Filtering**, click **Custom Filters**.

3 Do one of the following:

— To enable a filter, select the check box next to the desired filter and then click **Enable**.

— To disable a filter, select the appropriate check box and then click **Disable**.

Importing a Custom Filters File

You can choose to import a hand-coded custom filters file instead of using the Custom Filters Editor. You should be thoroughly familiar with the Sieve programming language (`http://www.faqs.org/rfcs/rfc3028.html`). Before you import and enable your hand-coded custom filters file, refer to the Administration Guide appendix on Sieve coding (Appendix A, “Creating Filters by Coding in Sieve,” on page 129) to ensure that your filters conform to Brightmail’s implementation for Sieve.

To import a Custom Filters file:

1 In the Brightmail Control Center, click the **Settings** tab.

2 In the left pane, under **Content Filtering**, click **Custom Filters**.

3 Click **Use a custom filters file** and then click **Browse**.

4 In the dialog box, choose your custom filters file.

5 In the Brightmail Control Center, click **Import**.

The Brightmail Control Center transmits the file and instructs all Brightmail Servers to load it.

Details About Custom Filters

Keep the following in mind when you create custom filters:

- Unless the Brightmail software is in communication with an MTA that is deployed at the border of the Internet (your gateway), the envelope domain or IP address on a message checked by the `Envelope Helo Domain` or `Peer IP` test may be the internal

domain that passed on the message from the email gateway, rather than the Internet address you might expect.

- To start out, you may want to set your policies so that messages that match against custom filters are quarantined, forwarded, or modified instead of deleted. When you are sure the custom filters are working correctly, you can adjust the action.
- If you accepted the default installation directories, the custom filters you create are stored in a file called:
  - `C:\Program Files\Brightmail\Config\sieve_script.txt` (Windows)
  - `/opt/brightmail/sieve_script.txt` (UNIX)

  This file is coded in the Sieve language. For a generalized description of Sieve, visit the site `http://www.faqs.org/rfcs/rfc3028.html`. Differences between the RFC3028 version of Sieve and the implementation available in the Brightmail software are described in "Creating Filters by Coding in Sieve," on page 129.
- You can manually edit the Sieve code created by Brightmail AntiSpam, but if you run the editor in the Brightmail Control Center again, your manual changes will be overwritten.
- You cannot configure Brightmail AntiSpam to check messages against a combination of custom filters created in the Brightmail Control Center and a manually created custom filters file.
- If you created Sieve scripts without using the Brightmail Control Center, such as for previous versions of Brightmail AntiSpam, you have two options. You may recreate the behavior of the Sieve scripts using the Custom Filters Editor, or you may continue to use a text editor to create new or edit existing Sieve scripts.

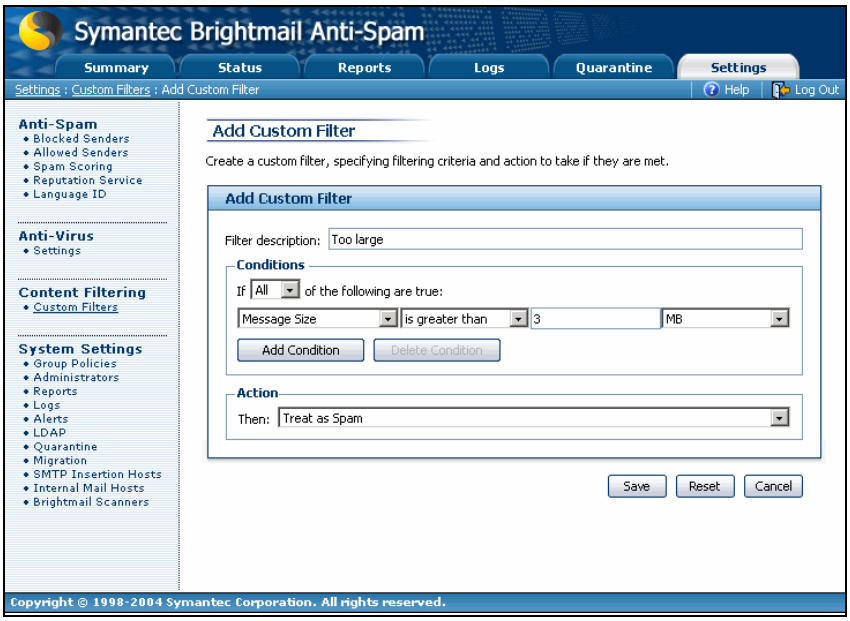
Sample Custom filters

Following are examples of custom filters that you can configure in the Brightmail Control Center. Because a limited number of characters are visible in the text fields in the Custom Filters Editor, the text in the pages below appears to be truncated. However, you can type more characters than are visible in the text fields.

To set actions for messages matching custom filters, see "Managing Group Policies," on page 33.

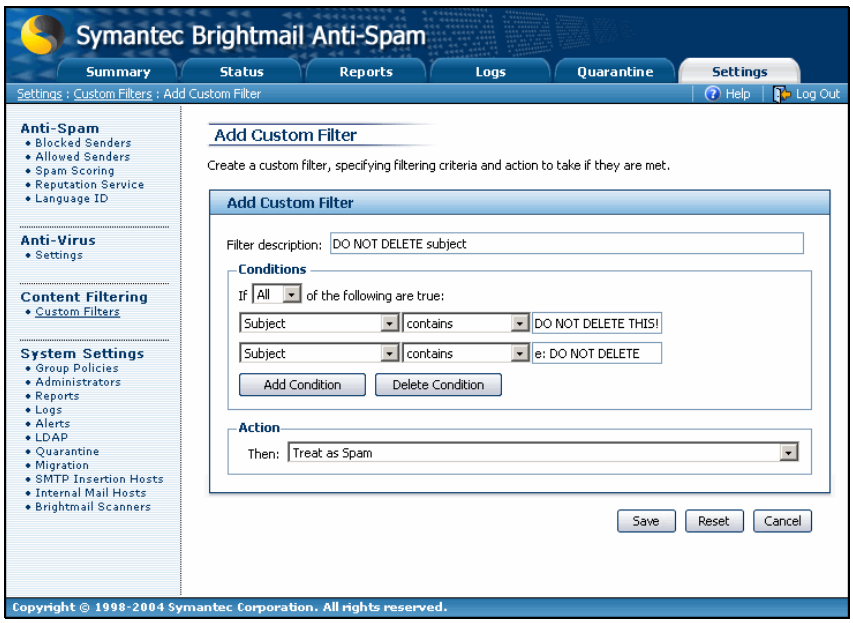
Intercept large messages

This example sets a match for any email message larger than three megabytes.



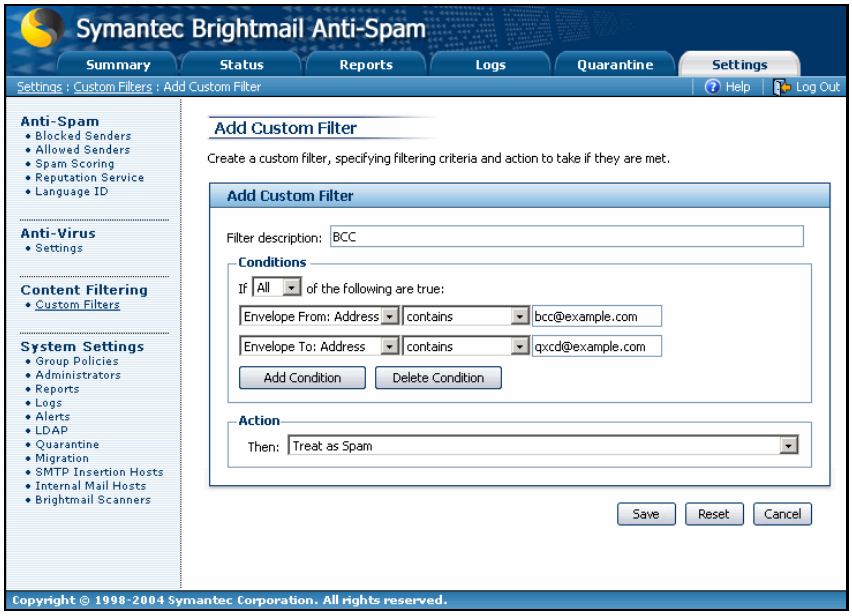
Intercept messages with a specific subject line

This example catches a message with a specific subject line, such as a chain letter.



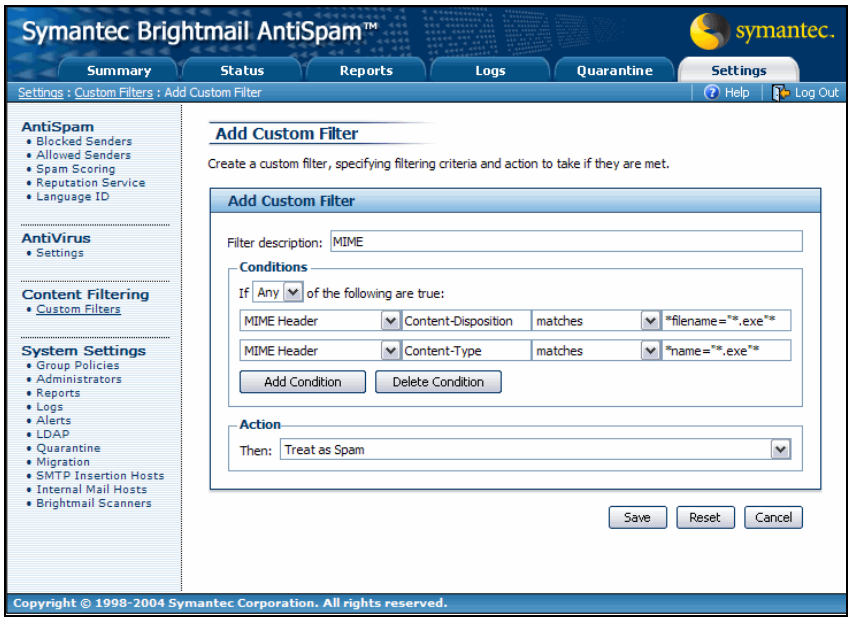
Intercept messages based on the sender and recipient

This example intercepts messages from a specific sender sent to a specific recipient. The example uses the `Envelope From Address` and `Envelope To Address` components because these are harder to forge than the `From` and `To` headers.



Intercept messages with a specific MIME type

This example intercepts messages that have a MIME attachment ending in `.exe`.



Creating Reports

This section describes how to set up and run reports. The following topics are covered here:

- Available Reports
- Setting the Retention Period for Reporting Data
- Choosing Data to Track
- Running Reports
- Understanding the Report Presentation
- Saving Reports
- Printing Reports
- Scheduling Reports

Symantec Brightmail AntiSpam reporting capabilities provide you with information about filtering activity at your site. With Symantec Brightmail AntiSpam reports, you can:

- Analyze consolidated filtering performance for all Brightmail Scanners and investigate spam and virus attacks targeting your organization.
- Create several pre-defined reports that track useful information, such as which domains are the source of most spam and which recipients are the top targets of spammers.
- Export report data for use in any reporting or spreadsheet software for further analysis.
- Schedule reports to be emailed at specified intervals.

You run, schedule, and customize reports from the Brightmail Control Center.

Available Reports

By default, Symantec Brightmail AntiSpam keeps track of the following totals over all Brightmail Scanners for the time period that you specify:

- Messages processed by a given Brightmail Scanner
- Spam messages detected
- Suspected spam messages detected, based on your Spam Scoring settings

- Total blocked messages, based on the entries in your Blocked Senders List
- Total allowed messages, based on the entries in your Allowed Senders List
- False positives, or possibly legitimate messages that a Brightmail Scanner has identified as spam
- Total viruses and worms

The following table shows the names of pre-set reports that you can generate and their contents. The third column lists the reporting data that you must instruct Brightmail to track before you can generate the specified report. You can choose from a selection of reports, all of which can be customized to include specific date ranges, time period groupings, email delivery, and a choice of comma separated value (CSV) or HTML output options. For some reports, you can filter based on specific recipients and senders of interest.

Table 12. Available Spam and Virus Reports

Report Type:	Displays...	Required Report Data Storage Options (Reports Settings Page)
`Mail Summary`	A summary of total mail.	None.
Spam Reports		
`Detection`	A summary of total *detected messages* (spam, blocked, allowed and suspected spam messages). Also reports false positives.	None
`Top Sender Domains`	The domain names of the senders of detected messages.	Sender domains
`Top Senders`	The email addresses of the top senders of filtered messages.	Senders
`Specific Senders`	Detected messages filtered by specific senders that you specify	Senders
`Top Sender HELO Domains*`	Domain names of the `SMTP HELO` servers from which messages have been received.	Sender HELO domains
`Top Sender IP Connections*`	The top IP connections from which spam has been received.	Senders
`Top Recipients Domains`	The domain names of the recipients of detected messages.	Recipient Domains
`Specific Recipients`	The filtering activity for specific email addresses that you choose.	Recipients
`Top Recipients`	The email addresses of the top recipients of detected messages.	Recipients
Virus Reports		
`Detection`	A summary of total viruses and worms.	None

Table 12. Available Spam and Virus Reports (Continued)

Report Type:	Displays...	Required Report Data Storage Options (Reports Settings Page)
`Top Sender Domains`	The domain names of the senders of viruses and worms.	Senders Sender domains
`Top Senders`	The email addresses of the top senders of viruses and worms.	Senders Sender domains
`Specific Senders`	Number of viruses and worms by senders that you specify.	Senders Sender domains
`Top Sender HELO Domains`*	Domain names of the `SMTP HELO` servers from which viruses and worms have been received.	Sender HELO domains
`Top Sender IP Connections`*	The top IP connections from which viruses and worms have been received.	Senders Sender domains
`Top Recipients Domains`	The domain names of the recipients of viruses and worms.	Recipient Domains
`Specific Recipients`	The filtering activity for specific email addresses that you choose.	Recipients
`Top Recipients`	The email addresses of the top recipients of viruses and worms.	Recipients

* If you are running any Brightmail Scanners in internal relay configurations, the `SMTP HELO` name or IP connection address could be the name or connection of your gateway machine, rather than the Internet address you might expect.

NOTE: *Before choosing to store data for reports, see the Symantec Brightmail AntiSpam Deployment Planning Guide for sizing information on the disk storage requirements of different types of reports. Because the data storage requirements for some reports can be high, refer to* "Setting the Retention Period for Reporting Data," on page 72 *to learn how to keep the report data manageable.*

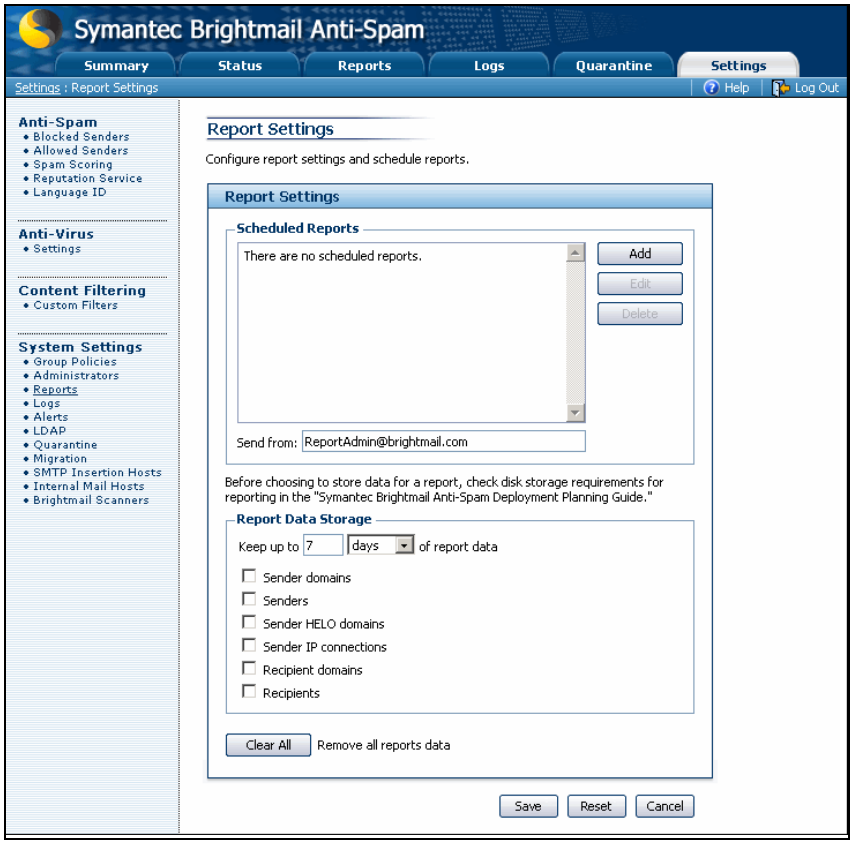
Setting the Retention Period for Reporting Data

You can specify the number of days, weeks, or months that Brightmail AntiSpam should keep track of reports data. Depending on your organization's size and message volume, the disk storage requirements for reports data could be quite large. You should monitor the storage required for reporting over time and adjust the retention period accordingly. See the *Symantec Brightmail AntiSpam Deployment Planning Guide* for guidelines on report storage requirements.

To specify the number of days, weeks, or months that Brightmail AntiSpam keeps track of reporting data:

1 In the Brightmail Control Center, click the **Reports** tab, and then click **Settings**.

The Reports Settings page is displayed.



2 Change the number of days, weeks, or months that Brightmail AntiSpam keeps track of your reporting data.

3 Click **Save.**

Choosing Data to Track

By default, Brightmail AntiSpam tracks data for two basic reports: `Spam: Detection` and `Virus: Detection`. Before you can generate other reports, you must configure Brightmail AntiSpam to track and store data appropriate for the report. For example, to generate recipient-based reports, such as `Spam/Virus: Specific Recipients`, you must configure Brightmail AntiSpam to store recipient information. See Table 12, "Available Spam and Virus Reports," on page 70 for a list of reports and the data you must store for each type of report.

To enable data tracking for reports:

1. In the Brightmail Control Center, click the **Reports** tab.
2. Click **Settings**.
3. Under **Reports Data Storage**, select the report data you want to track.
4. Click **Save**.

   Brightmail AntiSpam will begin to store the specified report data.

Running Reports

Provided that report data exists to generate a given report type, you can run an ad hoc report to get a summary of filtering activity. The results will display in the browser window.

To run a report:

1. Ensure that you have configured Brightmail AntiSpam to track the appropriate data for the report. See "Choosing Data to Track," on page 73 for more information.
2. In the Brightmail Control Center, click the **Reports** tab.

   The Reports page is displayed.

3. In the **Report Filter** section, select a report from the **Report Type** list.
4. In the **Time Range** list, do one of the following:
   - To specify a preset range, select **Past Hour**, **Past Day**, **Past Week**, and **Past Month**.

— To specify a different time period, select **Customize**, and then click in the **Start Date** and **End Date** fields and use the pop calendar to graphically select a time range. You must have JavaScript enabled in your browser to use the calendar.

5 In the **Group By** list, select **Hour**, **Day**, **Week**, or **Month**.

6 For reports that rank results, such as `Spam: Top Senders`, specify the number of entries you want to display per group.

7 For reports that filter on specific recipients, such as `Spam: Specific Recipients` or `Virus: Specific Recipients`, type the email addresses in the **Recipients** or **Sender** box. Separate multiple senders or recipients with spaces, commas, or semi colons.

Some tips on specifying addresses:

— To match on `user_1@domain.com`, you can use fully qualified email addresses (`user_1@domain.com`) or you can use the alias alone (`user_1`).

— If a user name matches more than one email address (for example, `user_1@domain1.com` and `user_1@domain2.com`), all addresses with that alias will be shown in the report.

8 Click **Run Report**.

If there is data available, the report you selected appears in the browser window.

Depending on how much data is available for the report you selected, this may take up to several minutes.

9 Optional: Click **Print Report**, **Save as HTML**, or **Save as CSV** (Comma Separated Values).

Troubleshooting Report Generation

Instead of displaying the expected reports, Brightmail AntiSpam might display the following message:

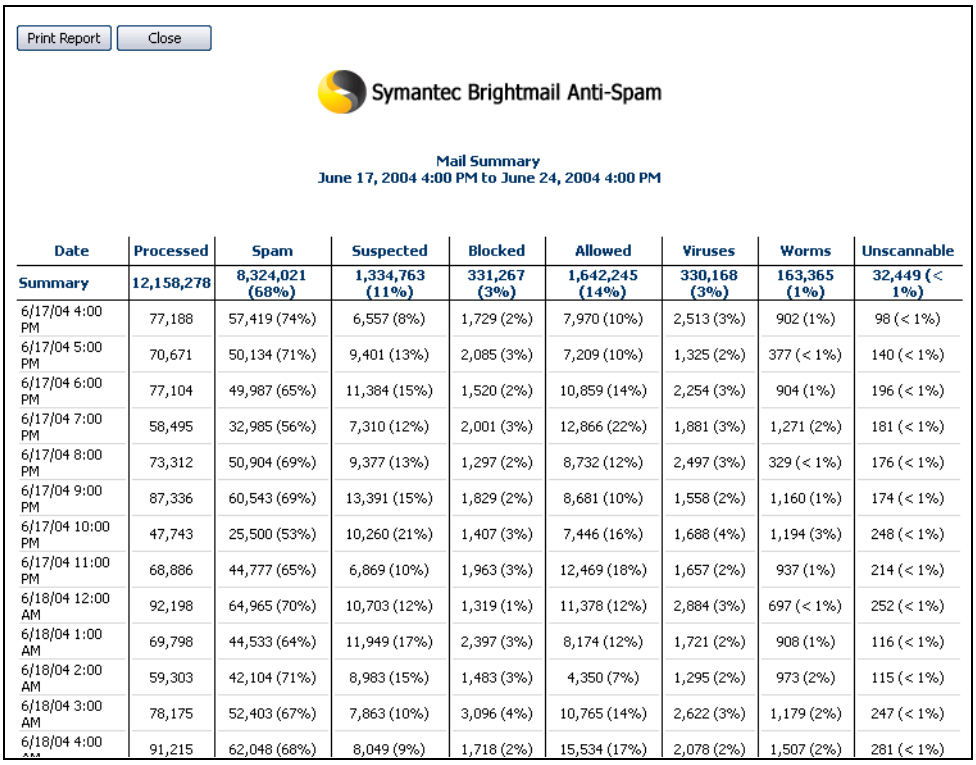
```
No data for the specified parameters
```

If you received this message, verify the following:

- **Data exists for the filter you specified –** For example, perhaps you specified a recipient address that didn't receive any mail over the specified period when generating a Specific Recipients report
- **Brightmail AntiSpam is configured to keep data for that report type –** See "Choosing Data to Track," on page 73 for more information. Keep in mind that occasionally you will be able to produce reports even if you are not currently tracking data. This will happen if you were collecting data in the past and then turned off data tracking. The data collected will be available for report generation until they are old enough to be automatically purged. After that period, report generation will fail. The **Keep for** *x* **days setting** on the Report Settings page controls this retention period.

Understanding the Report Presentation

The following figure shows a typical report.



Print Report | Close

Symantec Brightmail Anti-Spam

Mail Summary
June 17, 2004 4:00 PM to June 24, 2004 4:00 PM

Date	Processed	Spam	Suspected	Blocked	Allowed	Viruses	Worms	Unscannable
Summary	12,158,278	8,324,021 (68%)	1,334,763 (11%)	331,267 (3%)	1,642,245 (14%)	330,168 (3%)	163,365 (1%)	32,449 (< 1%)
6/17/04 4:00 PM	77,188	57,419 (74%)	6,557 (8%)	1,729 (2%)	7,970 (10%)	2,513 (3%)	902 (1%)	98 (< 1%)
6/17/04 5:00 PM	70,671	50,134 (71%)	9,401 (13%)	2,085 (3%)	7,209 (10%)	1,325 (2%)	377 (< 1%)	140 (< 1%)
6/17/04 6:00 PM	77,104	49,987 (65%)	11,384 (15%)	1,520 (2%)	10,859 (14%)	2,254 (3%)	904 (1%)	196 (< 1%)
6/17/04 7:00 PM	58,495	32,985 (56%)	7,310 (12%)	2,001 (3%)	12,866 (22%)	1,881 (3%)	1,271 (2%)	181 (< 1%)
6/17/04 8:00 PM	73,312	50,904 (69%)	9,377 (13%)	1,297 (2%)	8,732 (12%)	2,497 (3%)	329 (< 1%)	176 (< 1%)
6/17/04 9:00 PM	87,336	60,543 (69%)	13,391 (15%)	1,829 (2%)	8,681 (10%)	1,558 (2%)	1,160 (1%)	174 (< 1%)
6/17/04 10:00 PM	47,743	25,500 (53%)	10,260 (21%)	1,407 (3%)	7,446 (16%)	1,688 (4%)	1,194 (3%)	248 (< 1%)
6/17/04 11:00 PM	68,886	44,777 (65%)	6,869 (10%)	1,963 (3%)	12,469 (18%)	1,657 (2%)	937 (1%)	214 (< 1%)
6/18/04 12:00 AM	92,198	64,965 (70%)	10,703 (12%)	1,319 (1%)	11,378 (12%)	2,884 (3%)	697 (< 1%)	252 (< 1%)
6/18/04 1:00 AM	69,798	44,533 (64%)	11,949 (17%)	2,397 (3%)	8,174 (12%)	1,721 (2%)	908 (1%)	116 (< 1%)
6/18/04 2:00 AM	59,303	42,104 (71%)	8,983 (15%)	1,483 (3%)	4,350 (7%)	1,295 (2%)	973 (2%)	115 (< 1%)
6/18/04 3:00 AM	78,175	52,403 (67%)	7,863 (10%)	3,096 (4%)	10,765 (14%)	2,622 (3%)	1,179 (2%)	247 (< 1%)
6/18/04 4:00 AM	91,215	62,048 (68%)	8,049 (9%)	1,718 (2%)	15,534 (17%)	2,078 (2%)	1,507 (2%)	281 (< 1%)

The **Processed** column in the report shows the total number of messages processed. Each of the columns to the right of **Processed** shows the number of messages in one of seven categories, and the percent that category represents of the total messages processed.

Reports presented in local time of Control Center

Brightmail AntiSpam stores statistics in the `stats` directory on the individual hosts that run Brightmail Scanners. As in previous versions of Brightmail AntiSpam, the date and hour for each set of these statistics are recorded in Greenwich Mean Time (GMT). In this version of Brightmail AntiSpam, a single Brightmail Control Center that is connected to all the Brightmail Scanners generates reports that represent *all* the connected hosts. The combined numbers from all Brightmail Scanners in the reports are presented in the local time zone of the Brightmail Control Center.

Although the reports themselves do not list times—they only list a date—you should be aware of the implications of the GMT/local time conversion. The boundaries for splitting the reporting data into groups of days, weeks, or months are set from the perspective of the Brightmail Control Center.

For example, during the summertime, California is 7 hours behind GMT. Assume that a Brightmail Scanner receives and marks a message as spam at 5:30pm local time on April

23, Friday (12:30am, April 24, Saturday GMT). When generating the report, Brightmail AntiSpam determines what day the email belongs to based on where the report is being generated. If the Brightmail Control Center is in Greenwich, the resulting report will count it in GMT (the local time zone) so it will increase the spam count for April 24. If the Brightmail Control Center is in San Francisco, California, the report will count it in Pacific Daylight Time (the local time zone), and will accordingly increase the spam count for April 23.

See the following URL to translate GMT into your local time:
`http://www.timeanddate.com/worldclock/converter.html`

By default, data are saved for one week

By default, statistics are retained for seven days. If Brightmail AntiSpam already has seven days of data, the oldest hour of statistics will be deleted as each new hour of statistics is stored. To keep the data longer, see "Setting the Retention Period for Reporting Data," on page 72.

Statistics are recorded per message delivery, not per message

For example, if a single email lists 12 recipients, that email will be delivered to all 12. Therefore, it will increase the processed count by 12 for that day. If this message is spam, it will also increase the spam count by 12 for that day. Note that if you run a `Spam: Specific Recipients` report in this situation and list one of the 12 recipients, both the processed count and the spam count for that recipient will only have increased by 1.

Virus Messages double-counted when Clean and Deliver action is selected

For virus reports, if the AntiVirus Cleaner is configured to deliver clean mail to the same instance of the MTA that is running Brightmail AntiSpam, the virus message will be double-counted in the Processed total in the virus report. It will be counted one time for the original virus message and another time for the cleaned message.

Reports limited to 1,000 rows

The maximum size for any report, including a scheduled report, is 1,000 rows.

Saving Reports

Once you create a report in the Brightmail Control Center, you can save the report. You can save the results in a Web-based format, such as HTML. You can export the report to a comma-delimited format, suitable for importing into spreadsheet or database applications.

To save a report:

1. After creating a report as described in "Running Reports," on page 73, click **Save as HTML** or **Save as CSV** (buttons only appear if there is data for the specified report parameters).

2 A file dialog box appears for you to save the report in a location of your choice.

NOTE: *If you are using Netscape 7.1 and your browser is saving exported .csv reports with a .do extension, set the Helper Application MIME type correctly in Netscape Preferences.*

Printing Reports

After creating a report as described in "Running Reports," on page 73, click **Print View**.

The current report is displayed in a new browser window. Click **Print Report** to display the print dialog box for your operating system. The **Print Report** and **Close** buttons are hidden when you print the report by clicking **Print Report**.

Scheduling Reports

You can schedule some reports to run automatically at specified intervals. You can specify that scheduled reports be emailed to one or more recipients.

Reports that filter based on specific senders or recipients (`Spam: Specific Senders`, `Spam: Specific Recipients`, `Virus: Specific Senders`, `Virus: Specific Recipients`) cannot be scheduled.

To schedule a report:

1 Ensure that you have configured Brightmail AntiSpam to track the appropriate data for the report. See "Choosing Data to Track," on page 73 for more information.

2 In the Brightmail Control Center, click the **Reports** tab, and then click **Settings**.

3 Under **Scheduled Reports**, click **Add**.

4 In the **Scheduled Reports** section of the **Add Scheduled Reports** page, select a report from the **Report type** list.

5 In the **Group by** list, select **Hour, Day**, **Week**, or **Month**.

6 In the **Top entries to display** box, specify the number entries you want to display per group.

7 In the **Time range** list, select **Past Hour**, **Past Day**, **Past Week**, or **Past Month**.

8 In the **Report Generation Time** section, specify the time at which you want to generate the report.

9 Based on the reporting interval you want, do one of the following:

— To schedule daily reports, click **Daily**, and then click **Every day** or **Weekdays only**.

— To schedule weekly reports, click **Weekly**, and then click any combination of days.

— To schedule monthly reports, click **Monthly**, and then specify a day of the month or click **Last day of every month**.

10 Under **Report Format**, click one of the following to specify the format:

— **HTML** formats the report in HTML format.

— **CSV** formats the report in comma-separated-values format

11 Under **Report Destination**, enter at least one email address in the **Send to the following email addresses** box. You can use spaces, commas, or semi-colons as separators between email addresses to facilitate cutting and pasting addresses from email clients.

12 Click **Save**.

13 In the **Send from** box on the **Report Settings** page, type the email address from which reports should appear to be sent.

14 Click **Save**.

To edit a scheduled report:

1 In the Brightmail Control Center, click the **Reports** tab, and then click **Settings**.

2 Under **Scheduled Reports**, click the check box next to the scheduled report that you want to edit, and then click **Edit**. You can also click the underlined report name to jump directly to the edit page for the report.

3 Make any changes to the settings.

4 Click **Save**.

To delete a scheduled report:

1 In the Brightmail Control Center, click the **Reports** tab, and then click **Settings**.

2 Under **Scheduled Reports**, click the check boxes next to any reports that you want to delete, and then click **Delete**

Working with Brightmail Quarantine

Brightmail Quarantine provides storage of spam messages and Web-based end-user access to spam. You can also configure Brightmail Quarantine for administrator-only access. Use of Brightmail Quarantine is optional. Brightmail Quarantine is installed on the same computer as the Brightmail Control Center. This section includes the following topics:

- Using LDAP for End User Access to Quarantine
- Working with Messages in Quarantine for Administrators
- Working with Messages in Quarantine for End Users
- Configuring Quarantine
- Administering Quarantine

Using LDAP for End User Access to Quarantine

If you want users on your network to view their messages in Quarantine, you must configure Quarantine to access an LDAP directory such as Active Directory or Sun ONE Directory Server as described in this section. If you don't have an LDAP directory or don't want users to access Quarantine, you can configure Quarantine for administrator-only access—see "Configuring Quarantine for Administrator-Only Access," on page 102.

Configuring Quarantine for Active Directory

The following steps describe how to configure Quarantine to allow users specified in Active Directory to log in and access their spam messages.

To configure Quarantine to access Active Directory:

1. In the Brightmail Control Center, click the **Settings** tab, and then click **LDAP**.
2. In the **Server** box, type the fully qualified domain name or IP address of an Active Directory domain controller, such as `dc.example.com`. If you have a multi-domain Active Directory forest, specify the fully qualified domain name or IP address of the Global Catalog server on the root domain. See "Determining Fully Qualified Domain Names on Windows," on page 82 if you aren't sure what to type in the **Server** box.

3 In the **Port** box, type the TCP/IP port for the Active Directory server listed in the **Server** box. Usually the port will be 389, the default port for LDAP servers.

4 In the **Type** list, click **Active Directory** if it isn't already displayed.

5 Under **LDAP Server Login**, choose **Anonymous bind** or **Use the following** to specify a user name and password.

- **Anonymous bind**: Unless you've configured Active Directory to allow anonymous access, the **Anonymous bind** setting does not usually have adequate authentication privileges for Quarantine to access the necessary Active Directory information.
- **Use the following:** Type the user name and password for an account that can authenticate as an administrator. Specify the user name as *`NetBIOS\user name`*, such as `MSALPHA\Administrator`. See "Determining NetBIOS Names on Windows," on page 82 if you aren't sure what to type for the *`NetBIOS`* portion of the login information. The **Name** and **Password** boxes cannot be empty. Choose **Anonymous Bind** to specify empty **Name** and **Password** boxes.

NOTE: *If you are connecting to an Active Directory forest, specify an administrator that has administrative privileges across the domains you specify in the Windows Domain Settings box.*

6 Click **Test Login** to verify that Quarantine can authenticate against Active Directory using the information you've supplied so far.

If the test is successful, text similar to the following is displayed at the top of the page. Continue with the next step.

```
Test login to LDAP server successful.
```

If the test is unsuccessful, the following is displayed. Double check the information you've specified. Don't proceed until clicking **Test Login** yields positive results.

```
Test login to LDAP server failed.
```

7 In the **Windows Domain Names** box, type the NetBIOS domain names used by Active Directory. If you have multiple domains, separate them with a semicolon. See "Determining NetBIOS Names on Windows," on page 82 to determine the NetBIOS names for your domains. For example:

```
MSALPHA;MSBETA
```

If you specify multiple domains, users must choose the appropriate NetBIOS domain from a list on the login page when they log in to Quarantine.

8 Click **Auto Fill** to fill in the boxes below using the information you've already supplied.

9 Click **Test Query** to determine if Quarantine can access the required user information using the settings filled in after you clicked **Auto Fill**.

If the test is successful, text similar to the following is displayed at the top of the page. The maximum number of returned users per specified base DN is 1000 in this test. If you have more than 1000 users in your directory server, you will see a message like:

```
Query results
DC=yourdomain,DC=com - 1000+ Users
```

If the test is unsuccessful, an error message describing the problem is displayed. For example, if the **Query start** and/or **Query filter** are missing, a message like the following is displayed.

```
For testing query, please specify Start and Filter attributes.
```

Modify the appropriate settings and continue with the next step.

10 If the test query was successful but the response time is slow or your site has multiple domains, modify the **Query start (base DN)**. Make your Base DN as specific as possible to make queries faster, such as by specifying the CN or OU. For example:

```
CN=users,DC=msalpha,DC=com

          or

OU=Marketing,DC=msalpha,DC=com
```

If you have multiple OU's or domains, list each separated by an ampersand, such as:

```
DC=msalpha,DC=com&DC=msbeta,DC=com

          or

CN=Users,DC=msalpha,DC=com&OU=Marketing,DC=msbeta,DC=com

          or

CN=Users,DC=msalpha,DC=com&OU=Marketing,DC=msbeta,
DC=com&OU=Sales,DC=msbeta,DC=com
```

11 If the Test Query was unsuccessful, you may need to modify one or more of the following settings from the defaults provided when you click **Fill Settings Below**.

— **Query filter**: The **Query filter** must include the values from **User login name attribute**, **Primary email attribute**, and **Email alias attribute** as wildcard searches. These values are filled in when you click **Auto Fill**. The default value for Active Directory is:

```
(&(|(objectCategory=group)(objectCategory=person))(&(|(mail=*)
(proxyAddresses=*))(sAMAccountName=*)))
```

- — **User login name attribute**: The default value for Active Directory is: `sAMAccountName`
- — **Primary email attribute**: The default value for Active Directory is: `mail`
- — **Email alias attribute**: The default value for Active Directory is: `proxyAddresses`

12 Click **Save** to save the settings on this page.

You've successfully completed the LDAP settings for Quarantine. Be sure to click **Save** and then attempt to log in to Quarantine as a user that exists in Active Directory. See "Logging In," on page 13.

Determining Fully Qualified Domain Names on Windows

Follow this step if you need to determine the fully qualified domain name for your Active Directory domains.

- Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Active Directory Domains and Trusts**.

  The fully qualified domain name is listed on the left side of the window.

Determining NetBIOS Names on Windows

Follow these steps if you need to determine the NetBIOS name for your Active Directory domains.

To determine the NetBIOS name for your Active Directory domains:

1 Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Active Directory Domains and Trusts**.

2 Select an Active Directory domain from the left side of the window.

3 Click **Action** and then click **Properties**.

  The value in the "Domain name (pre-Windows 2000)" box is the NetBIOS name for the selected domain.

Configuring a Global Catalog to Work With Quarantine

To configure Quarantine to access a Global Catalog, specify the port for the Global Catalog, usually 3268, in the LDAP Settings page in Quarantine. In addition, verify that the nCName attribute is replicated to the Global Catalog.

To replicate the nCName attribute to the Global Catalog using the Active Directory Schema snap-in:

1 Click **Start**, click **Run**, type `regsvr32 schmmgmt.dll` and click **OK**.

2 Click **Start**, click **Run**, type **mmc** and click **OK**.

3 On the **File** menu, click **Add/Remove Snap-in**.

4 Click **Add** and select **Active Directory Schema** from the list.

5 In the left pane, expand **Active Directory Schema**, and click **Attributes**.

6 In the right pane, locate and double-click the **nCName** attribute.

7 Select the **Replicate this attribute** to the **Global Catalog** check box.

If an error occurs after performing the steps above, make sure that the current domain controller has permission to modify the schema.

To grant permission to the current domain controller:

1 Open the Active Directory Schema snap-in as described above.

2 In the left pane, click **Active Directory Schema** to select it.

3 On the **Action** menu, click **Operations Master**.

4 Click the check box for **The Schema may be modified on this Domain Controller**.

If replication to the Global Catalog cannot be modified as described above, contact your Symantec representative for a work-around.

Required Exchange 5.5 Settings for Quarantine Compatibility

Ensure that Exchange 5.5 is configured as described below so Quarantine can access the user data stored in Exchange 5.5.

- In the Exchange 5.5 user properties, Mailbox nickname (alias) should always match the NT account name.
- In the Exchange 5.5 LDAP Protocol Settings, modify the number for "Maximum Number of Search Results Returned" to be 1000 or to be greater than the maximum number of entries expected to be returned by the Query Filter. This number can **not** exceed 1000 as that is the limit imposed by Quarantine. This setting only impacts the Brightmail Control Center LDAP Setting **Test Query** operation and not authentication or email alias resolution.

Configuring Quarantine for Exchange 5.5

The following steps describe how to configure Quarantine to allow users specified in Exchange 5.5 to log in and access their spam messages.

To configure Quarantine to access Exchange 5.5 directory information:

1 In the Brightmail Control Center, click the **Settings** tab, and then click **LDAP**.

2 In the **Server** box, type the fully qualified domain name or IP address of an Exchange 5.5 server.

3 In the **Port** box, type the TCP/IP port for the Active Directory server listed in the **Server** box. Usually the port will be 389, the default port for LDAP servers.

4 In the **Type** list, click **Exchange 5.5** if it isn't already displayed.

5 Under **LDAP Server Login**, choose **Anonymous bind** or **Use the following** to specify a user name and password.

— **Anonymous bind**: Unless you've configured Exchange 5.5 to allow anonymous access, the **Anonymous bind** setting does not usually have adequate authentication privileges for Quarantine to access the necessary Exchange 5.5 information.

— **Use the following**: Type the user name and password for an account that can authenticate as an administrator, for example, `cn=Administrator,cn=yourdomain`

The **Name** and **Password** boxes cannot be empty. Choose **Anonymous Bind** to specify empty **Name** and **Password** boxes.

6 Click **Test Login** to verify that Quarantine can authenticate against Exchange 5.5 using the information you've supplied so far.

If the test is successful, text similar to the following is displayed at the top of the page. Continue with the next step.

```
Test login to LDAP server successful.
```

If the test is unsuccessful, the following is displayed. Double check the information you've specified. Don't proceed until clicking **Test Login** yields positive results.

```
Test login to LDAP server failed.
```

7 Leave the **Windows Domain Names** box blank.

8 Click **Auto Fill** to fill in the boxes below using the information you've already supplied.

9 Click **Test Query** to determine if Quarantine can access the required user information using the settings filled in after you clicked **Auto Fill**.

If the test is successful, text similar to the following is displayed at the top of the page. The maximum number of returned users per specified base DN is 1000 in this test. If you have more than 1000 users in your directory server, you will see a message like:

```
Query results
DC=yourdomain,DC=com - 1000+ Users
```

If the test is unsuccessful, an error message describing the problem is displayed. For example, if the **Query start** and/or **Query filter** are missing, a message like the following is displayed.

```
For testing query, please specify Start and Filter attributes.
```

Modify the appropriate settings and continue with the next step.

10 If the test query was successful but the response time is slow or your site has multiple domains, modify the **Query start (base DN)**. Make your Base DN as specific as possible to make queries faster, such as by specifying the CN or OU. For example:

```
CN=users,DC=msalpha,DC=com

          or

OU=Marketing,DC=msalpha,DC=com
```

If you have multiple OU's or domains, list each separated by an ampersand, such as:

```
DC=msalpha,DC=com&DC=msbeta,DC=com

          or

CN=Users,DC=msalpha,DC=com&OU=Marketing,DC=msbeta,DC=com

          or

CN=Users,DC=msalpha,DC=com&OU=Marketing,DC=msbeta,
DC=com&OU=Sales,DC=msbeta,DC=com
```

11 If the Test Query was unsuccessful, you may need to modify one or more of the following settings from the defaults provided when you click Fill Settings Below.

— **Query filter**: The **Query filter** must include the values from **User login name attribute**, **Primary email attribute**, and **Email alias attribute** as wildcard searches. These values are filled in when you click **Auto Fill**. The default value for Exchange 5.5 is:

`(&(|(objectClass=groupOfNames)(objectClass=organizationalPerson))(|(mail=*)(otherMailbox=*)))`

— **User login name attribute**: The default value for Exchange 5.5 is:

`mail` (Primary mail address)

— **Primary email attribute**: The default value for Exchange 5.5 is:

`mail`

— **Email alias attribute**: The default value for Exchange 5.5 is:

`otherMailbox`

12 Click **Save** to save the settings on this page.

You've successfully completed the LDAP settings for Quarantine. Be sure to click Save and then attempt to log in to Quarantine as a user that exists in Exchange 5.5. See "Logging In," on page 13.

Configuring Quarantine for iPlanet/Sun ONE/Java Directory Server

The following steps describe how to configure Quarantine to allow users specified in iPlanet, Sun ONE, or Java Directory Server to log in and access their spam messages.

To configure Quarantine to access iPlanet/Sun ONE Directory Server:

1. In the Brightmail Control Center, click the **Settings** tab, and then click **LDAP**.
2. In the **Server** box, type the fully qualified domain name or IP address of the LDAP server, such as `ldap.example.com`.
3. In the **Port** box, type the TCP/IP port for the LDAP server listed in the **Server** box. Usually the port will be 389, the default port for LDAP servers.
4. In the **Type** list, click **iPlanet/Sun ONE/Java Directory Server**.
5. Under **LDAP Server Login**, choose **Anonymous bind** or **Use the following** to specify a user name and password.
   - **Anonymous bind**: Unless you've configured LDAP to allow anonymous access, this setting does not usually have adequate authentication privileges for Quarantine to access the necessary LDAP information.
   - **Use the following:** Type the user name and password for an account that can authenticate as an administrator. For iPlanet, Sun ONE, or Java Directory Server, the default administrator is `cn=Directory Manager`. The **Name** and **Password** boxes cannot be empty. Choose **Anonymous Bind** to specify empty **Name** and **Password** boxes.
6. Click **Test Login** to verify that Quarantine can authenticate against LDAP using the information you've supplied so far.

   If the test is successful, text similar to the following is displayed at the top of the page. Continue with the next step.

   ```
   Test login to LDAP server successful.
   ```

   If the test is unsuccessful, the following is displayed. Double check the information you've specified. Don't proceed until clicking **Test Login** yields positive results.

   ```
   Test login to LDAP server failed.
   ```

   Leave the **Windows Domain Names** box blank.
7. Click **Auto Fill** to fill in the boxes below using the information you've already supplied.
8. Click **Test Query** to determine if Quarantine can access the required user information using the settings filled in after you clicked **Auto Fill**.

   If the test is successful, text similar to the following is displayed at the top of the page. The maximum number of returned users per specified base DN is 1000 in this test. If you have more than 1000 users in your directory server, you will see a message like:

   ```
   Query results
   DC=yourdomain,DC=com - 1000+ Users
   ```

If the test is unsuccessful, an error message describing the problem is displayed. For example, if the **Query start** and/or **Query filter** are missing, a message like the following is displayed.

```
For testing query, please specify Start and Filter attributes.
```

Modify the appropriate settings and continue with the next step.

9 If the Test Query was successful but the response time is slow, or your site has multiple domains, modify the **Query start (base DN)**. Make your Base DN as descriptive as possible to make queries faster, such as by specifying the CN or OU. For example:

```
CN=users,DC=ldapalpha,DC=com
          or
OU=Marketing,DC=ldapalpha,DC=com
```

If you have multiple OU's or domains, list each separated by an ampersand, such as:

```
DC=ldapalpha,DC=com&DC=ldapbeta,DC=com
          or
CN=Users,DC=ldapalpha,DC=com&OU=Marketing,DC=ldapbeta,DC=com
          or
CN=Users,DC=ldapalpha,DC=com&OU=Marketing,DC=ldapbeta,
DC=com&OU=Sales,DC=ldapbeta,DC=com
```

10 If the Test Query was unsuccessful, you may need to modify one or more of the following settings from the defaults provided when you click **Auto Fill**.

— **Query filter**: The **Query filter** must include the values from **User login name attribute**, **Primary email attribute**, and **Email alias attribute** as wildcard searches. These values are filled in when you click **Auto Fill**. The default value for Sun ONE Directory Server is:

```
(&(|(objectClass=inetMailGroup)(objectClass=person))(|(mail=*)
(mailalternatedaddress=*)))
```

— **User login name attribute**: The default value for Sun ONE Directory Server is:

```
mail
```

— **Primary email attribute**: The default value for Sun ONE Directory Server is:

```
mail
```

— **Email alias attribute**: The default value for Sun ONE Directory Server is:

```
mailAlternateAddress
```

11 Click **Save** to save the settings on this page.

You've successfully completed the LDAP settings for Quarantine. Attempt to log in to Quarantine as a user that exists in the iPlanet or Sun ONE Directory Server. See "Logging In," on page 13.

Configuring Quarantine for Other LDAP Servers

Quarantine can be configured to access LDAP servers other than Active Directory, Sun ONE Directory Server, or Exchange 5.5. The following steps provide guidelines for configuring Quarantine to allow users specified in a your LDAP Server to log in and access their spam messages.

NOTE: *If using OpenLDAP as an LDAP server, make sure it is configured to accept LDAP v2 protocol requests.*

To configure Quarantine to access an alternate LDAP Server:

1. In the Brightmail Control Center, click the **Settings** tab, and then click **LDAP**.
2. In the **Server** box, type the fully qualified domain name or IP address of the LDAP server, such as `ldap.example.com`.
3. In the **Port** box, type the TCP/IP port for the LDAP server listed in the **Server** box. Usually the port will be 389, the default port for LDAP servers.
4. In the **Type** list, click **Other**.
5. Under **LDAP Server Login**, choose **Anonymous bind** or **Use the following** to specify a user name and password.
   - **Anonymous bind**: Unless you've configured LDAP to allow anonymous access, this setting does not usually have adequate authentication privileges for Quarantine to access the necessary LDAP information.
   - **Use the following:** Type the user name and password for an account that can authenticate as an administrator. The **Name** and **Password** boxes cannot be empty. Choose **Anonymous Bind** to specify empty **Name** and **Password** boxes.
6. Click **Test Login** to verify that Quarantine can authenticate against LDAP using the information you've supplied so far.

   If the test is successful, text similar to the following is displayed at the top of the page. Continue with the next step.

   ```
   Test login to LDAP server successful.
   ```

   If the test is unsuccessful, the following is displayed. Double check the information you've specified. Don't proceed until clicking **Test Login** yields positive results.

   ```
   Test login to LDAP server failed.
   ```

   Leave the **Windows Domain Names** box blank.

7 Click **Auto Fill** to fill in the boxes below using the information you've already supplied.

8 Click **Test Query** to determine if Quarantine can access the required user information using the settings filled in after you clicked **Auto Fill**.

If the test is successful, text similar to the following is displayed at the top of the page. The maximum number of returned users per specified base DN is 1000 in this test. If you have more than 1000 users in your directory server, you will see a message like:

```
Query results
DC=yourdomain,DC=com - 1000+ Users
```

If the test is unsuccessful, an error message describing the problem is displayed. For example, if the **Query start** and/or **Query filter** are missing, a message like the following is displayed.

```
For testing query, please specify Start and Filter attributes.
```

Modify the appropriate settings and continue with the next step.

9 If the Test Query was successful but the response time is slow, or your site has multiple domains, modify the **Query start (base DN)**. Make your Base DN as descriptive as possible to make queries faster, such as by specifying the CN or OU. For example:

```
CN=users,DC=ldapalpha,DC=com

          or

OU=Marketing,DC=ldapalpha,DC=com
```

If you have multiple domains, list each domain separated by an ampersand, such as:

```
DC=ldapalpha,DC=com&DC=ldapbeta,DC=com

          or

CN=Users,DC=ldapalpha,DC=com&OU=Marketing,DC=ldapbeta,DC=com

          or

CN=Users,DC=ldapalpha,DC=com&OU=Marketing,DC=ldapbeta,
DC=com&OU=Sales,DC=ldapbeta,DC=com
```

10 If the Test Query was unsuccessful, you may need to modify one or more of the following settings from the defaults provided when you click **Auto Fill**.

- — **Query filter**: The **Query filter** must include the values from **User login name attribute**, **Primary email attribute**, and **Email alias attribute** as wildcard searches. These values are filled in when you click **Auto Fill**. The default value is:

  ```
  (&(|(objectClass=inetMailGroup)(objectClass=person))(|(mail=*)
  (mailalternatedaddress=*)))
  ```

- — **User login name attribute**: The default is `mail`
- — **Primary email attribute**: Specify a single-valued attribute holding the primary email address.
- — **Email alias attribute**: Specify a single-valued attribute holding the alias email address.

11 Click **Save** to save the settings on this page.

You've successfully completed the LDAP settings for Quarantine. Attempt to log in to Quarantine as a user that exists in the LDAP Server. See "Logging In," on page 13.

Working with Messages in Quarantine for Administrators

Accessing Quarantine

Administrators access Quarantine by logging into the Brightmail Control Center. All administrators can work with messages in Quarantine. Administrators without full privileges or Manage Quarantine rights won't see the **Quarantine** link in the **Settings** tab, and the **Settings** button will be grayed out.

Users access Quarantine by logging into the Brightmail Control Center using the user name and password required by the type of LDAP server employed at your company. For users, the Quarantine message list page is displayed after logging in.

Administrator Message List Page

The administrator message list page provides a summary of the messages in Quarantine. The user message list page is very similar. See "Differences Between the Administrator and User Message List Pages," on page 92 for more information.

Sorting Messages

By default, messages are listed in date descending order, meaning that the newest messages are listed at the top of the page. Click on the **To**, **From**, **Subject**, or **Date** column heading to select the column by which to sort. A triangle appears in the selected column that indicates ascending or descending sort order. Click on the selected column heading to toggle between ascending and descending sort order.

Viewing Messages

Click on a message subject to view an individual message.

Redelivering Misidentified Messages

Very rarely, you may see messages in Quarantine that are not spam. Click on the check box to the left of a misidentified message and then click **This is not Spam** to redeliver the message to the intended recipient. This also removes the message from Quarantine. Depending on how you configured Quarantine, a copy of the message may also be sent to an administrator email address (such as yourself), Brightmail, or both. This allows the email administrator and/or Brightmail to monitor the effectiveness of the Symantec Brightmail AntiSpam software.

Deleting Individual Messages

Click on the check box to the left of each message to select a message for deletion. When you've selected all the messages on the current page that you want to delete, click **Delete**.

Deleting a message in the administrator's Quarantine also deletes the message from the applicable user's Quarantine. For example, if you delete Kathy's spam messages in the administrator's Quarantine, Kathy won't be able to see those messages when accessing Quarantine.

Deleting All Messages

Click **Delete All** to delete all the messages in Quarantine, including those on other pages. Click **OK** in the confirmation window or **Cancel** if you've changed your mind. This deletes all users' spam messages.

Searching Messages

Click **Search** to search messages for a specific recipient, sender, subject, message ID, or date range. See "Searching Messages," on page 94.

Navigating Through Messages

Table 13 describes ways to navigate through message list pages.

Table 13. Navigating Through Messages on the Administrator Message List Page

Button	Description
	Go to beginning of messages
	Go 50 pages ahead. This button is displayed if there are 50 pages or more of messages after the current page.
	Go to the end of messages. This button is displayed if there are less than 50 pages of messages after the current page.
	Go to previous page of messages

Table 13. Navigating Through Messages on the Administrator Message List Page (Continued)

Button	Description
	Go to next page of messages
	Choose up to 50 pages before or after the current page of messages

Configuring Settings

Click the **Settings** button to configure settings for Quarantine. To return to the message list from the settings area, click the **Quarantine** tab. See "Configuring Quarantine," on page 101.

Administrator Message List Page Details

Note the following Quarantine behavior:

- When you navigate to a different page of messages, the status of the check boxes in the original page is not preserved. For example, if you select three messages in the first page of messages and then move to the next page, when you return to the first page, all the message check boxes are cleared again.
- The "To" column in the message list page indicates the intended recipient of each message as listed in the message envelope. When you display the contents of a single message in the message details page, the To header (not envelope) information is displayed, which is often forged by spammers.

Differences Between the Administrator and User Message List Pages

The pages displayed for administrators and other users on your network have some differences.

- Users can only view and delete their own spam messages. Quarantine administrators can view and delete all users' spam messages, either one by one, deleting all messages, or deleting the results of a search.
- When users click **This Is Not Spam**, the message is delivered to their own main inbox. When a Quarantine administrator clicks **This Is Not Spam**, the message is delivered to the inbox of the intended recipient.
- The administrator message list page includes a "To" column containing the intended recipient of each message. Users can only see their own messages, so the "To" column is unnecessary.
- The **Settings** button is only available to Quarantine administrators, not users.
- Users only have access to Quarantine, not the rest of the Brightmail Control Center.

Administrator Message Details Page

When you click on the subject line of a message in the message list page, this page displays the contents of individual spam messages. The user message details page is very similar. See "Differences Between the Administrator and User Message Pages," on page 94 for more information.

Redelivering Misidentified Messages

Like the button on the message list page, you can click **This is not Spam** to redeliver the message to the intended recipient. This also removes the message from Quarantine. Depending on how you've configured Quarantine, a copy of the message may also be sent to the email administrator (you), Brightmail, or both. This allows you and/or Brightmail to monitor the effectiveness of the Symantec Brightmail AntiSpam software.

Deleting the Message

To delete the message currently being viewed, click **Delete**.

When you delete a message, the page refreshes and displays the next message. If there are no more messages, the message list page is displayed.

Deleting a message in the administrator's Quarantine also deletes the message from the applicable user's Quarantine. For example, if you delete Kathy's spam messages in the administrator's Quarantine, Kathy won't be able to see those messages when accessing Quarantine.

Navigating Through Messages

Table 14 describes ways to navigate messages.

Table 14. Navigating Through Messages on the Administrator Message Details Page

Button	Description
Next	Go to next message
Previous	Go to previous message

Returning to the Message List

To return to the message list, click **Back To Messages**.

Displaying Full or Brief Headers

By default, the From, To, Subject, and Date headers of a message are displayed. To display all headers available to Quarantine, click **Display Full Headers**. The full headers may provide clues about the origin of a message, but keep in mind that spammers usually forge some of the message headers. To hide the full headers, click **Display Brief Headers**.

Configuring Settings

Click the **Settings** tab to configure settings for Quarantine. To return to the message list from the settings area, click the **Quarantine** tab. See "Configuring Quarantine," on page 101.

Graphics Appear as Gray Rectangles

When viewed in Quarantine, the original graphics in messages are replaced with graphics of gray rectangles. This suppresses offensive images and prevents spammers from verifying your email address. If you release the message by clicking **This is not Spam**, the original graphics will be viewable by the intended recipient. It is not possible to view the original graphics within Quarantine.

Attachments

The names of attachments are listed at the bottom of the message, but the actual attachments can't be viewed from within Quarantine. However, if you redeliver a message by clicking **This is not Spam**, the message and attachments will be accessible from the inbox of the intended recipient.

Differences Between the Administrator and User Message Pages

The pages displayed for administrators and other users on your network have some differences.

- Users can only view and delete their own spam messages. Quarantine administrators can view and delete messages for all users.
- Users only have access to Quarantine, not the rest of the Brightmail Control Center.

Searching Messages

Click **Search** on the message list page to display the search page. Type in one or more boxes or choose a time range to display matching messages in the administrator Quarantine. The search results are displayed in a page similar to the message list page.

The user search page is very similar. See "Differences Between the Administrator and User Search Pages," on page 96 for more information.

Searching Using Multiple Characteristics

If you search for multiple characteristics, only messages that match the combination of characteristics are listed in the search results. For example, if you typed "LPQTech" in the From box and "Inkjet" in the Subject box, only messages containing "LPQTech" in the From header and "Inkjet" in the Subject header would be listed in the search results.

Searching Message Envelope "To" Recipient

Type in the **To** box to search the message envelope RCPT TO recipient in all messages for the text you typed. You can search for a display name, the user name portion of an email address, or any part of a display name or email user name. If you type a full email address

in the **To** box, only the user name portion of `user_name@example.com` is searched for. You can attempt to search for the domain portion of an email address by typing just the domain, but if more than 50% of the messages contain part of the search phrase, nothing will be displayed (see "Search Details," on page 95). The search is limited to the envelope To, which may contain different information than the header To displayed on the message details page.

Searching "From" Headers

Type in the **From** box to search the From header in all messages for the text you typed. You can search for a display name, email address, or any part of a display name or email address. The search is limited to the visible message From header, which in spam messages is usually forged. The visible message From header may contain different information than the message envelope.

Searching Subject Headers

Type in the **Subject** box to search the Subject header in all messages for the text you typed.

Searching the Message ID Header

Type in the **Message ID** box to search the message ID in all messages for the text you typed.

The message ID is not visible in Quarantine, but it can obtained by examining the mail log on the MTA. In addition, most email clients have the capability of displaying the full message header which includes the message ID. For example, in Outlook 2000, double click on a message to show it in a window by itself, click **View** and then click **Options**.

The message ID is typically assigned by the first email server to receive the message and is supposed to be a unique identifier for a message. However, spammers may tailor the message ID to suit their purposes, such as to hide their identity. For legitimate email, the message ID may indicate the domain where the message was sent from and/or the email server used to send the message.

Searching Using Time Range

Choose a time range from the **Time Range** list to show all messages from that time range. You can also choose **Customize** to search using specific time range.

Search Details

Note the following search behavior:

- **If any term in the search phrase matches 50% or more of the messages in the database, then the search will show no results.**
- About 570 common words such as "after" and "which" are ignored in any of the search boxes, as well as the word "spam". These are called MySQL stopwords. Also, words of three characters or less are ignored. This applies to To, From, Subject, and Message ID searches.

- If any word in a multiple word search is found in a message, that message is considered a match. For example, searching for “red carpet” will match “red carpet,” and also “red wine” and “flying carpet.” You don’t have to put quote marks around search text that contains spaces.
- Searches match exact whole words only in To, From, Subject, and Message ID searches. A word is considered a group of letters, numbers, or underscores. For example, if you searched for “finance”, the search would not find “refinance”. Also, if you searched for “user_name@example.com”, the search is interpreted as “user_name” OR “example”. Since “com” is three characters, it is ignored. The @ and the period are treated as spaces.
- Search results are sorted by date descending order by default but can be resorted by clicking on a column heading.
- Wildcards such as * are not supported in search. All searches are literal.
- If you search for multiple characteristics, only messages that match the combination of characteristics are listed in the search results. For example, if you typed “LPQTech” in the From box and “Inkjet” in the Subject box, only messages containing “LPQTech” in the From header and “Inkjet” in the Subject header would be listed in the search results.
- All text searches are case-insensitive. This means that if you typed `emerson` in the From box, then messages with a From header containing `emerson`, `Emerson`, and `eMERSOn` would all be displayed in the search results.
- The amount of time required for the search is dependent on how many search boxes you filled in and the number of messages in the current mailbox. Searching in the administrator mailbox will take longer than searching in a user’s mailbox.
- Spammers usually “spoof” or forge some of the visible messages headers such as From and To and the invisible envelope information. Sometimes they forge header information using the actual email addresses or domains of innocent people or companies.

Differences Between the Administrator and User Search Pages

- Quarantine administrators can search for recipients.
- In the Search Results page, users can only delete their own spam messages. Quarantine administrators can delete all users’ spam messages.

Working with Messages in Quarantine for End Users

Message List Page

The message list page is the first page displayed when you log in and provides a summary of the messages in Quarantine.

Sorting Messages

By default, messages are listed in date descending order, meaning that the newest messages are listed at the top of the page. Click on the **To**, **From**, **Subject**, or **Date** column heading to select the column by which to sort. A triangle appears in the selected column that indicates ascending or descending sort order. Click on the selected column heading to toggle between ascending and descending sort order.

Viewing Messages

Click on a message subject to view an individual message.

Redelivering Misidentified Messages

Very rarely, you may see messages in Quarantine that are not spam. Click on the check box to the left of a misidentified message and then click **This is not Spam** to redeliver the message to your usual inbox. This also removes the message from Quarantine. Depending on how your email administrator configured Quarantine, a copy of the message may also be sent to the email administrator, Brightmail, or both. This allows the email administrator and/or Brightmail to monitor the effectiveness of the Symantec Brightmail AntiSpam software.

Deleting Individual Messages

Click on the check box to the left of each message to select a message for deletion. When you've selected all the messages on the current page that you want to delete, click **Delete**.

Deleting All Messages

Click **Delete All** to delete all the messages in your Quarantine mailbox, including those on other pages. Click **OK** in the confirmation window or **Cancel** if you've changed your mind.

Searching Messages

Click **Search** to search messages for a specific sender, subject, message ID, or date range. See "Searching Messages," on page 99.

Navigating Through Messages

Table 15 describes ways to navigate through message list pages.

Table 15. Navigating Through Messages on the End User Message List Page

Button	Description
	Go to beginning of messages
	Go 50 pages ahead. This button is displayed if there are 50 pages or more of messages after the current page.

Table 15. Navigating Through Messages on the End User Message List Page (Continued)

Button	Description
	Go to the end of messages. This button is displayed if there are less than 50 pages of messages after the current page.
	Go to previous page of messages
	Go to next page of messages
	Choose up to 50 pages before or after the current page of messages

Message List Page Details

Note the following Quarantine behavior:

- When you navigate to a different page of messages, the status of the check boxes in the original page is not preserved. For example, if you select three messages in the first page of messages and then move to the next page, when you return to the first page, all the message check boxes are cleared again.

Message Details Page

When you click on the subject line of a message in the message list page, this page displays the contents of individual spam messages.

Redelivering Misidentified Messages

Like the button on the message list page, you can click **This is not Spam** to redeliver the message to your usual inbox. This also removes the message from Quarantine. Depending on how your email administrator configured Quarantine, a copy of the message may also be sent to the email administrator, Brightmail, or both. This allows you and/or Brightmail to monitor the effectiveness of the Symantec Brightmail AntiSpam software.

Deleting the Message

To delete the message currently being viewed, click **Delete**.

When you delete a message, the page refreshes and displays the next message. If there are no more messages, the message list page is displayed.

Navigating Through Messages

Table 16 describes ways to navigate messages.

Table 16. Navigating Through Messages on the End User Message Details Page

Button	Description
Next	Go to next message
Previous	Go to previous message

Returning to the Message List

To return to the message list, click **Back To Messages**.

Displaying Full or Brief Headers

By default, the From, To, Subject, and Date headers of a message are displayed. To display all headers available to Quarantine, click **Display Full Headers**. The full headers may provide clues about the origin of a message, but keep in mind that spammers usually forge some of the message headers. To hide the full headers, click **Display Brief Headers**.

Graphics Appear as Gray Rectangles

When viewed in Quarantine, the original graphics in messages are replaced with graphics of gray rectangles. This suppresses offensive images and prevents spammers from verifying your email address. If you release the message by clicking **This is not Spam**, you can view the original graphics when the message is delivered to your main inbox. It is not possible to view the original graphics within Quarantine.

Attachments

The names of attachments are listed at the bottom of the message, but the actual attachments can't be viewed from within Quarantine. However, if the message is misidentified spam, when you redeliver it by clicking **This is not Spam**, the message and attachments will be accessible from your main inbox.

Searching Messages

Click **Search** on the message list page to display the search page. Type in one or more boxes or choose a time range to display matching messages in your Quarantine mailbox. The search results are displayed in a page similar to the message list page.

Searching Using Multiple Characteristics

If you search for multiple characteristics, only messages that match the combination of characteristics are listed in the search results. For example, if you typed "LPQTech" in the From box and "Inkjet" in the Subject box, only messages containing "LPQTech" in the From header and "Inkjet" in the Subject header would be listed in the search results.

Searching “From” Headers

Type in the **From** box to search the From header in all messages for the text you typed. You can search for a display name, email address, or any part of a display name or email address. The search is limited to the visible message From header, which in spam messages is usually forged. The visible message From header may contain different information than the message envelope.

Searching Subject Headers

Type in the **Subject** box to search the Subject header in all messages for the text you typed.

Searching the Message ID Header

Type in the **Message ID** box to search the message ID in all messages for the text you typed.

The message ID is not visible in Quarantine, but it can obtained by examining the mail log on the MTA. In addition, most email clients have the capability of displaying the full message header which includes the message ID. For example, in Outlook 2000, double click on a message to show it in a window by itself, and then click **View** and then click **Options**.

The message ID is typically assigned by the first email server to receive the message and is supposed to be a unique identifier for a message. However, spammers may tailor the message ID to suit their purposes, such as to hide their identity. For legitimate email, the message ID may indicate the domain where the message was sent from and/or the email server used to send the message.

Searching Using Time Range

Choose a time range from the **Time Range** list to show all messages from that time range. You can also choose **Customize** to search using specific time range.

Search Details

Note the following search behavior:

- **If any term in the search phrase matches 50% or more of the messages in the database, then the search will show no results.**
- About 570 common words such as “after” and “which” are ignored in any of the search boxes, as well as the word “spam”. These are called MySQL stopwords. Also, words of three characters or less are ignored. This applies to To, From, Subject, and Message ID searches.
- If any word in a multiple word search is found in a message, that message is considered a match. For example, searching for “red carpet” will match “red carpet,” and also “red wine” and “flying carpet.” You don’t have to put quote marks around search text that contains spaces.

- Searches match exact whole words only in From, Subject, and Message ID searches. A word is considered a group of letters, numbers, or underscores. For example, if you searched for “finance”, the search would not find “refinance”. Also, if you searched for “user_name@example.com”, the search is interpreted as “user_name” OR “example”. Since “com” is three characters, it is ignored. The @ and the period are treated as spaces.
- Search results are sorted by date descending order by default but can be resorted by clicking on a column heading.
- Wildcards such as * are not supported in search. All searches are literal.
- If you search for multiple characteristics, only messages that match the combination of characteristics are listed in the search results. For example, if you typed “LPQTech” in the From box and “Inkjet” in the Subject box, only messages containing “LPQTech” in the From header and “Inkjet” in the Subject header would be listed in the search results.
- All text searches are case-insensitive. This means that if you typed `emerson` in the From box, then messages with a From header containing `emerson`, `Emerson`, and `eMERSOn` would all be displayed in the search results.
- The amount of time required for the search is dependent on how many search boxes you filled in and the number of messages in the current mailbox.
- Spammers usually “spoof” or forge some of the visible messages headers such as From and To and the invisible envelope information. Sometimes they forge header information using the actual email addresses or domains of innocent people or companies.

Configuring Quarantine

Delivering Messages to Quarantine from the Brightmail Server

Use the Group Policies filtering actions to deliver spam messages to Quarantine from Brightmail Server.

NOTE: *Quarantine does not use a separate SMTP mail server to send notifications and resend misidentified messages, although an SMTP mail server must be available to receive notifications and misidentified messages sent by Quarantine. Set this SMTP server on the* ***SMTP Insertion Settings*** *page. The SMTP server you choose should be downstream from the Brightmail Server, as notifications and misidentified messages do not require filtering.*

To deliver messages to Quarantine:

1. In the Brightmail Control Center, click the **Settings** tab, and then click **Group Policies**.
2. Under **Groups**, click the appropriate group, such as **Default**.

3 Under **AntiSpam Actions**, set the filtering action to **Quarantine the Message** for the desired spam types. Typically, you'll want to set **If a message is spam** and **If a message is suspected spam** to **Quarantine the Message**.

4 Click **Save**.

5 Repeat this process for each group policy that you want to set to deliver messages to Quarantine.

For more information about Group Policies, see "Managing Group Policies," on page 33.

Configuring Quarantine for Administrator-Only Access

If you don't have an LDAP directory server configured or don't want users in your LDAP directory to access Quarantine, you can configure Quarantine so that only administrators can access the messages in Quarantine.

When administrator-only access is enabled, you can still perform all the administrator tasks described in "Working with Messages in Quarantine for Administrators," on page 90, including redelivering misidentified messages to local users, whether or not you're using an LDAP directory at your organization. However, notification of new spam messages is disabled when administrator-only access is enabled.

To configure Quarantine for administrator-only access:

1 In the Brightmail Control Center, click the **Settings** tab.

2 In the left pane, under **System Settings**, click **Quarantine.**

3 Select the check box for **Administrator-only Quarantine.**

4 Click **Save**.

Configuring the User and Distribution List Notification Digests

By default, a notification process runs at 4 a.m. every day and determines if users have new spam messages in Quarantine since the last time the notification process checked. If so, it sends a message to users who have new spam to remind them to check their spam messages in Quarantine. You can also choose to send notification digests to users on distribution lists. The sections below describe how to change the notification digest frequency and format.

Notification for Distribution Lists/Aliases

If Quarantine is enabled, a spam message sent to an alias with a one-to-one correspondence to a user's email address is delivered to the user's normal quarantine mailbox. For example, if `tom` is an alias for `tomevans`, quarantined messages sent to `tom` or to `tomevans` all arrive in the Quarantine account for `tomevans`.

NOTE: *An "alias" on UNIX or "distribution list" on Windows is an email address that translates to one or more other email addresses. In this text, distribution list is used to mean an email address that translates to two or more email addresses.*

When Symantec Brightmail AntiSpam forwards a spam message sent to a distribution list to Quarantine, the message is not delivered in the intended recipients' Quarantine. Instead, the message is delivered to a special Quarantine mailbox for that distribution list. However, you can configure Quarantine to send notification digests about the messages in a distribution list mailbox to the recipients of that distribution list by selecting the **Notify distribution lists** check box on the Quarantine Settings page. If the **Include View link** box is selected on the Quarantine Settings page, recipients of the notification digest can view all the quarantined distribution list messages. If a recipient clicks on the **This Is Not Spam** button for a message in the quarantined distribution list mailbox, the message is delivered to the normal inboxes of the distribution list recipients.

NOTE: *For example, if a distribution list called* `mktng` *contains* `ruth`, `fareed`, *and* `darren`, *spam sent to* `mktng` *and configured to be quarantined won't be delivered to the Quarantine inboxes for* `ruth`, `fareed`, *and* `darren`. *If the* ***Notify distribution lists*** *check box on the Quarantine Settings page is selected, then* `ruth`, `fareed`, *and* `darren` *will receive email notifications about the quarantined* `mkting` *messages. If the* ***Include View link*** *box is selected on the Quarantine Settings page, then* `ruth`, `fareed`, *and* `darren` *can view the quarantined* `mkting` *messages by clicking on the* ***View*** *link in the notification digests. If* `ruth` *clicks on the* ***This Is Not Spam*** *button for a quarantined* `mkting` *message, the message is delivered to the normal inboxes of* `ruth`, `fareed`, *and* `darren`.

Separate Notification Templates for Standard and Distribution List Messages

By default, the notification templates for standard quarantined messages and quarantined distribution list messages are different. This allows you to customize the notification templates for each type of quarantined message.

Changing the Notification Digest Frequency

To change the frequency at which notification messages are sent to users, follow the steps below. The default frequency is every day. To not send notification messages, change the Notification frequency to `NEVER`.

To change the notification digest frequency:

1. In the Brightmail Control Center, click the **Settings** tab.
2. In the left pane, under **System Settings**, click **Quarantine.**
3. Choose the desired setting from the **Notification frequency** list.
4. Click **Save**.

Changing the Notification Digest Templates

The notification digest templates determine the appearance of notification messages sent to users as well as the message subject and send from address.

The default notification templates are similar to the text listed below. The distribution list notification template lacks the information about logging in. In your browser, the text

doesn't wrap, so you'll have to scroll horizontally to view some of the lines. This prevents unusual line breaks or extra lines if you choose to send notifications in HTML format.

```
Quarantine Summary for %USER_NAME%

There are %NEW_MESSAGE_COUNT% new messages in your Spam Quarantine
since you received your last Spam Quarantine Summary. These messages
will automatically be deleted after %QUARANTINE_DAYS% days.

To review the complete text of these messages, go to %QUARANTINE_URL%
and log in.

==================== NEW QUARANTINE MESSAGES ====================

%NEW_QUARANTINE_MESSAGES%

=================================================================
```

In the notification digest sent to users, the variables in Table 17 are replaced with the information described in the Description column. You can reposition each variable in the template or remove it.

Table 17. Notification Message Variables

Variable	Description
%NEW_MESSAGE_COUNT%	Number of new messages in the user's Quarantine since the last notification message was sent.
%NEW_QUARANTINE_MESSAGES%	List of messages in the user's Quarantine since the last notification was sent. For each message, the contents of the From, Subject, and Date headers are printed. **View** and **Release** links are displayed for each message if they are enabled and you've chosen **Multipart** or **HTML** notification format.
%QUARANTINE_DAYS%	Number of days messages in Quarantine will be kept. After that period, messages will be purged.
%QUARANTINE_URL%	URL that the user clicks on to display the Quarantine login page.
%USER_NAME%	User name of user receiving the notification message.

To edit the notification templates, digest subject, and send from address:

1. In the Brightmail Control Center, click the **Settings** tab.
2. In the left pane, under **System Settings**, click **Quarantine.**
3. Under **Quarantine Notification**, click **Edit** next to **Notification templates**.
4. In the **Send from** box, type the email address that the notification digests should appear to be from. Since users can reply to the email address supplied, type an address where you can monitor users' questions about the notification digests. Specify the full email address including the domain name, such as `admin@example.com`.

5 In the **Subject** box, type the text that should appear in the Subject header of notification digests, such as "Your Suspected Spam Summary." Don't put message variables in the subject box; they won't be expanded.

NOTE: *The **Send from** and **Subject** settings will be the same for both the user notification template and distribution list notification template.*

6 Edit the user notification template, distribution list notification template, or both. See Table 17, "Notification Message Variables," on page 104. When viewed in the Control Center, the text doesn't wrap, so you'll have to scroll horizontally to edit some of the lines. This prevents unusual line breaks or extra lines if you choose to send notifications in HTML format. Don't manually insert breaks if you plan to send notifications in HTML.

7 Click **Save** to save your changes to the template and close the template editing window. Or, click one of the following:

- **Reset:** Discard changes to the notification template and leave the template editing window open.
- **Default:** Erase the current information and replace it with defaults.
- **Cancel:** Discard your changes to the notification template and close the template editing window.

8 Click **Save** in the **Quarantine Settings** page.

Enabling Notification for Distribution Lists

You can configure Quarantine to send notification digests about the messages in a distribution list mailbox to the recipients in a distribution list. See "Notification for Distribution Lists/Aliases," on page 102 for more information.

To enable notification for distribution lists:

1 In the Brightmail Control Center, click the **Settings** tab.

2 In the left pane, under **System Settings**, click **Quarantine.**

3 Under **Quarantine Notification**, select **Notify distribution lists**.

4 Click **Save** in the **Quarantine Settings** page.

Selecting the Notification Digest Format

The notification digest template determines the MIME encoding of the notification message sent to users as well as whether **View** and **Release** links appear in the message.

To choose a notification format:

1 In the Brightmail Control Center, click the **Settings** tab.

2 In the left pane, under **System Settings**, click **Quarantine.**

3 Under **Quarantine Notification**, click one of the following items in the **Notification formats** list:

- **Multipart (HTML and text):** Send a notification message in MIME multipart format. Users will see either the HTML version or the text version depending on the type of email client they are using and the email client settings. The **View** and **Release** links do not appear next to each message in the text version of the summary message.
- **HTML only:** Send the notification message in MIME type text/html only.
- **Text only:** Send the notification message in MIME type text/plain only. If you choose **Text only**, the **View** and **Release** links do not appear next to each message in the summary message.

4 Select the **Include View link** check box to include a **View** link next to each message in the notification digest message summary.

When a user clicks on the **View** link in a notification digest message, the adjacent message is displayed in Quarantine in the default browser. This check box is only available if you choose **Multipart (HTML and text)** or **HTML only** notification format**.** If you remove the `%NEW_QUARANTINE_MESSAGES%` variable from the notification digest template, the new message summary, including the **View** links, won't be available.

5 Select the **Include Release link** check box to include a **Release** link next to each message in the notification digest message summary.

The **Release** link is for misidentified messages. When a user clicks on the **Release** link in a notification digest message, the adjacent message is released from Quarantine and sent to the user's normal inbox. This check box is only available if you choose **Multipart (HTML and text)** or **HTML only** notification format**.** If you remove the `%NEW_QUARANTINE_MESSAGES%` variable from the notification digest template, the new message summary, including the **Release** links, won't be available.

6 Click **Save** in the **Quarantine Settings** page.

Configuring Recipients for Misidentified Messages

If users or administrators find false positive messages in Quarantine, they can click **This is not Spam**. Clicking **This is not Spam** redelivers the selected messages to the user's normal inbox. You can also send a copy to a local administrator, Brightmail, or both.

To configure recipients for misidentified message submissions:

1 In the Brightmail Control Center, click the **Settings** tab.

2 In the left pane, under **System Settings**, click **Quarantine.**

3 To report misidentified messages to Brightmail, select the **Brightmail Logistics and Operations Center (BLOC)** check box. It is selected by default.

The BLOC analyzes message submissions to determine if the Brightmail Filters need to be changed. However, the BLOC will not send confirmation of the misidentified message submission to the administrator or the user submitting the message.

4 To send copies of misidentified messages to a local administrator, select the **Administrator** check box under **Misidentified Messages** and type the appropriate

email address. These messages should be sent to someone who will monitor misidentified messages at your organization to determine the effectiveness of Brightmail AntiSpam.

Type the full email address including the domain name, such as `admin@example.com`. The administrator email address must not be an alias, or a copy of the misidentified message won't be delivered to the administrator email address, and errors will be recorded in the log accessible from the **Logs** tab (not the `BrightmailLog.log` Quarantine log file).

5 Click **Save** in the **Quarantine Settings** page.

Configuring the Delete Unresolved Email Setting

By default, quarantined messages sent to non-existent email addresses, based on LDAP lookup, will be deleted. If you clear the check box for **Delete messages sent to unresolved email addresses**, these messages will be stored in the Quarantine `postmaster` mailbox. "Checking the Quarantine Postmaster Mailbox," on page 111 describes how to view these messages.

NOTE: *If there is an LDAP server connection failure or LDAP settings have not been configured correctly, then quarantined messages addressed to non-existent users are stored in the Quarantine postmaster mailbox whether the* **Delete unresolved email** *check box is selected or cleared.*

Setting the Quarantine Message Retention Period

To change the amount of time spam messages are kept before being deleted, follow the steps below. You may want to shorten the retention period if quarantined messages are using too much of your system's disk space. However, a shorter retention period increases the chance that users may have messages deleted before they have been checked. The default retention period is 7 days.

By default, a Quarantine process runs at 1 a.m. every day to delete messages older than the retention period. Each time the process runs, at most 10,000 messages can be deleted. If your organization receives a very large volume of spam messages, contact your Symantec representative for instructions on how to change the deletion frequency.

To set the Quarantine Message Retention Period:

1 In the Brightmail Control Center, click the **Settings** tab.

2 In the left pane, under **System Settings**, click **Quarantine.**

3 Type the desired number of days in the **Days to store in Quarantine before deleting** setting.

4 Click **Save** in the **Quarantine Settings** page.

Configuring Messages Per Page in Quarantine

The **Messages to display per page** setting controls how many lines of messages display on the message list page for administrators and users. Larger numbers will cause the message list page to take longer to load.

To set the number of messages to display per page:

1. In the Brightmail Control Center, click the **Settings** tab.
2. In the left pane, under **System Settings**, click **Quarantine.**
3. Select the desired number in the **Messages to display per page** list.
4. Click **Save** in the **Quarantine Settings** page.

Configuring the Login Help

By default, when users click on the **Need help logging in?** link on the Brightmail Control Center login page, online help from Brightmail is displayed in a new window. You can customize the login help in two ways:

- Modify the contents of the existing login help page
- Specify a custom login help page

These changes only affect the login help page, not the rest of the online help. Both of these methods require knowledge of HTML.

To modify the contents of the existing login help page:

1. Open the following file in a text editor such as WordPad or vi:

```
.../Tomcat/jakarta-tomcat-4.1.27/webapps/brightmail/help/login_help_contents.jsp
...\Tomcat\jakarta-tomcat-4.1.27\webapps\brightmail\help\login_help_contents.jsp
```

2. Edit the `login_help_contents.jsp` file, using the existing contents as a guide. Although the filename extension is `.jsp`, the file is coded in HTML.
3. Save and exit from the `login_help_contents.jsp` file.

To specify a custom login help page:

1. Create a Web page that tells your users how to log in and make it available on your network. The Web page should be accessible from any computer where users will log in to Quarantine.
1. In the Brightmail Control Center, click the **Settings** tab.
2. In the left pane, under **System Settings**, click **Quarantine.**
3. In the **Login help URL** box, type the URL to the Web page you created.
4. Click **Save** in the **Quarantine Settings** page.

To disable your custom login help page, delete the contents of the **Login help URL** box.

Configuring the Quarantine Port for Incoming SMTP Email

By default, Quarantine accepts quarantined messages from Brightmail Scanner on port 41025. To specify a different port, type it in the **Quarantine Port** box. You don't need to change any Brightmail Scanner settings to match the change in the **Quarantine Port** box.

Specifying Quarantine Message and Size Thresholds

To limit the number of messages in Quarantine or size of Quarantine, configure Quarantine threshold settings.

Table 18. Quarantine Thresholds

Threshold	Description
Maximum size of quarantine database	Maximum amount of disk space used for quarantined messages for all users. When a new message arrives after the threshold has been reached, the 10 oldest messages are deleted, and the new message is kept.
Maximum size per user	Maximum amount of disk space used for quarantine messages per user. When a new message arrives after the threshold has been reached, the 10 oldest messages of the user are deleted, and the new message is kept.
Maximum number of messages	Maximum number of messages for all users (the same message sent to multiple recipients counts as one message). When a new message arrives after the threshold has been reached, the oldest message is deleted, and the new message is kept.
Maximum number of messages per user	Maximum number of quarantine messages per user. When a new message arrives after the threshold has been reached, the user's oldest message is deleted, and the new message is kept.

To specify Quarantine message and size thresholds:

1. In the Brightmail Control Center, click the **Settings** tab.
2. In the left pane, under **System Settings**, click **Quarantine.**
3. For each type of threshold you want to configure, select the check box and enter the size or message threshold. You can configure multiple thresholds.
4. Click **Save**.

NOTE: *No alert or notification occurs if Quarantine thresholds are exceeded. However, you can be alerted when disk space is low, which may be caused by a large number of messages in the Quarantine database. For more information about alerts, see* "Setting Up Event-Based Alerts," on page 121.

Administering Quarantine

Starting and Stopping Quarantine

The Installer configures Quarantine to start when the computer is turned on and to stop when the computer is shut down. However, there may be times when you need to manually stop and later start Quarantine processes, such as to investigate a problem on the computer where Quarantine is installed.

NOTE: *If you need to use the Tomcat commands in* `.../Tomcat/jakarta-tomcat-version/bin/`*, you must source the file* `/opt/brightmail/bmiq-env.sh` *to set* `JAVA_HOME` *and* `CATALINA_HOME`*. However, it's recommended to start and stop Tomcat using the commands below, which don't require sourcing* `bmiq-env.sh`.

To start Quarantine processes on UNIX:

To start Tomcat and related processes like the Expunger and Notifier, log in as root or use `sudo` to run the following command:

```
# /etc/init.d/tomcat4 start
Using CATALINA_BASE:   /opt/brightmail/Tomcat/jakarta-tomcat-4.1.27
Using CATALINA_HOME:   /opt/brightmail/Tomcat/jakarta-tomcat-4.1.27
Using CATALINA_TMPDIR: /opt/brightmail/Tomcat/jakarta-tomcat-4.1.27/
   temp
Using JAVA_HOME:       /opt/brightmail/jre
```

To start MySQL, log in as root or use `sudo` to run the following command:

```
# /etc/init.d/mysql.server start
# Starting mysqld daemon with databases from /opt/brightmail/MySQL/
   mysql-pro-4.0.16-sun-solaris2.8-sparc/data
```

To stop Quarantine processes on UNIX:

To stop MySQL, log in as root or use `sudo` to run the following command:

```
# /etc/init.d/mysql.server stop
Killing mysqld with pid NNNNN
Wait for mysqld to exit. done
```

To stop Tomcat and related processes like the Expunger and Notifier, log in as root or use `sudo` to run the following command:

```
# /etc/init.d/tomcat4 stop
Using CATALINA_BASE:   /opt/brightmail/Tomcat/jakarta-tomcat-4.1.27
Using CATALINA_HOME:   /opt/brightmail/Tomcat/jakarta-tomcat-4.1.27
Using CATALINA_TMPDIR: /opt/brightmail/Tomcat/jakarta-tomcat-4.1.27/
   temp
Using JAVA_HOME:       /opt/brightmail/jre
```

To start Quarantine services on Windows:

Follow these steps to start the Tomcat and MySql services. If a service has been stopped, the Status column in the **Services** window for that service is empty.

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Services**.
2. Navigate to and click **Tomcat**.
3. Click the Start Service triangle at the top of the **Services** window to start Tomcat.
4. Navigate to and click **MySql**.
5. Click the Start Service triangle at the top of the **Services** window to start MySql.
6. Close the **Services** window.

To stop Quarantine services on Windows:

Follow these steps to stop the MySql and Tomcat services. If a service is running, the Status column in the **Services** window for that service says "Started."

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Services**.
2. Navigate to and click **MySql**.
3. Click the Stop Service square at the top of the **Services** window to stop MySql.
4. Navigate to and click **Tomcat**.
5. Click the Stop Service square at the top of the **Services** window to stop Tomcat.

Close the **Services** window.

Checking the Quarantine Postmaster Mailbox

If Quarantine can't determine the proper recipient for a message received from Brightmail AntiSpam, it delivers the message to a `postmaster` mailbox accessible from Quarantine. Your network may also have a `postmaster` mailbox you access using a mail client that is separate from the Quarantine `postmaster` mailbox. Spam messages may also be delivered to the Quarantine `postmaster` mailbox if there is a problem with the LDAP configuration.

NOTE: *No notification messages are sent to the* `postmaster` *mailbox.*

To display messages sent to the `postmaster` mailbox:

1. Log into the Brightmail Control Center as an administrator with full privileges or Manage Quarantine rights.
2. Click **Quarantine**.
3. Click **Search**.
4. In the **To** box, type `postmaster`.
5. Click **Search**.

Checking the Quarantine Error Log

Periodically, you should check the Quarantine error log. All errors related to the Quarantine are written to the `BrightmailLog.log` file. The file is located in the Quarantine installation directory, which is usually in the directories listed below.

UNIX: `/opt/brightmail/ControlCenter/BrightmailLog.log`

Windows: `C:\Program Files\BrightmailAnti-Spam\BrightmailLog.log`

This file is a plain text file, viewable with a text editor such as Notepad or `vi`. Each problem results in a number of lines in the error log. For example, the following lines result when Quarantine receives a message too large to handle:

```
com.mysql.jdbc.PacketTooBigException: Packet for query is too large (3595207 >
   1048576)
at com.mysql.jdbc.MysqlIO.send(MysqlIO.java:1554)
at com.mysql.jdbc.MysqlIO.send(MysqlIO.java:1540)
at com.mysql.jdbc.MysqlIO.sendCommand(MysqlIO.java:1005)
at com.mysql.jdbc.MysqlIO.sqlQueryDirect(MysqlIO.java:1109)
at com.mysql.jdbc.Connection.execSQL(Connection.java:2030)
at com.mysql.jdbc.PreparedStatement.executeUpdate(PreparedStatement.java:1750)
at com.mysql.jdbc.PreparedStatement.executeUpdate(PreparedStatement.java:1596)
at org.apache.commons.dbcp.DelegatingPreparedStatement.executeUpdate
   (DelegatingPreparedStatement.java:207)
at com.brightmail.dl.jdbc.impl.DatabaseSQLManager.handleUpdate(Unknown Source)
at com.brightmail.dl.jdbc.impl.DatabaseSQLManager.handleUpdate(Unknown Source)
at com.brightmail.dl.jdbc.impl.DatabaseSQLTransaction.create(Unknown Source)
at com.brightmail.bl.bo.impl.SpamManager.create(Unknown Source)
at com.brightmail.service.smtp.impl.SmtpConsumer.run(Unknown Source)
```

Increasing the Amount of Logging Information in BrightmailLog.log for Debugging

If you have problems with Quarantine, you can increase the detail of the log messages saved into `BrightmailLog.log` by changing settings in the `log4j.properties` file. The `BrightmailLog.log` contains logging information for Quarantine and the Control Center. When you increase the logging level of `log4j.properties`, it creates a lot of log information, so it's recommended to increase the maximum size of the `BrightmailLog.log` as described below.

1 Open the following file in a text editor such as WordPad or vi:

`.../Tomcat/jakarta-tomcat-`*`version`*`/webapps/brightmail/WEB-INF/classes/log4j.properties`
`...\Tomcat\jakarta-tomcat-`*`version`*`\webapps\brightmail\WEB-INF\classes\log4j.properties`

2 Find the following line:

```
#log4j.rootLogger=ERROR, file
```

3 Change the word `ERROR` to `DEBUG`.

4 Find the following line:

```
log4j.appender.file.MaxFileSize=5MB
```

5 Change the `5MB` to the desired number, such as `10MB`.

6 Find the following line:

```
log4j.appender.file.MaxBackupIndex=10
```

7 Change the number after `MaxBackupIndex` to the desired number, such as 40.

This setting determines the number of saved `BrightmailLog.log` files. For example, if you specify 2, `BrightmailLog.log` contains the newest information, `BrightmailLog.log.1` contains the next newest, and `BrightmailLog.log.2` contains the oldest information. When `BrightmailLog.log` reaches the size indicated by `log4j.appender.file.MaxFileSize`, then it's renamed to `BrightmailLog.log.1`, and a new `BrightmailLog.log` file is created. The original `BrightmailLog.log.1 is renamed to BrightmailLog.log.2`, etc. This number times the value of `log4j.appender.file.MaxFileSize` determines the amount of disk space required for these logs.

8 Save and exit from the `log4j.properties` file.

NOTE: *Change the settings of the* `log4j.properties` *file back to the original settings when you're finished debugging Quarantine.*

Backing Up the Quarantine Message Database

The messages in Quarantine are stored in a MySQL database. See "Backing Up MySQL Data," on page 122 for information about how to back up and restore the Quarantine message database.

Troubleshooting

Message "The operation could not be performed." is Displayed

Rarely, you or users at your organization may see the following message displayed at the top of the Quarantine page while viewing email messages in Quarantine:

```
The operation could not be performed.
```

If this happens, check the Quarantine error log as described in "Checking the Quarantine Postmaster Mailbox," on page 111.

Can't Log in Due to Conflicting LDAP and Control Center Accounts

If there is an account in your LDAP directory with the user name of "`admin`," you won't be able to log in to Quarantine as that user, only as the Brightmail Control Center

administrator with that user name. The existing LDAP `admin` account conflicts with the default Control Center administrator, which is also `admin`.

To address this problem, you can change either the user name in LDAP or the user name of the Control Center administrator. Click the **Settings** tab, click **Administrators**, and then click **admin** to change the user name of the default Control Center administrator.

Error in Quarantine Log File Due to Very Large Spam Messages

If you check the Quarantine log file as described in "Checking the Quarantine Error Log," on page 112 and see lines similar to those listed below, the messages forwarded from Brightmail AntiSpam to Quarantine are larger than the standard packet size used by MySQL. If you see this error and expect to receive more large messages, you can configure the MySQL client and server to receive larger packets. See this Web page for more information `http://www.mysql.com/doc/en/Packet_too_large.html`:

```
com.mysql.jdbc.PacketTooBigException: Packet for query is too large (3595207 >
   1048576)
at com.mysql.jdbc.MysqlIO.send(MysqlIO.java:1554)
at com.mysql.jdbc.MysqlIO.send(MysqlIO.java:1540)
at com.mysql.jdbc.MysqlIO.sendCommand(MysqlIO.java:1005)
at com.mysql.jdbc.MysqlIO.sqlQueryDirect(MysqlIO.java:1109)
at com.mysql.jdbc.Connection.execSQL(Connection.java:2030)
at com.mysql.jdbc.PreparedStatement.executeUpdate(PreparedStatement.java:1750)
at com.mysql.jdbc.PreparedStatement.executeUpdate(PreparedStatement.java:1596)
at org.apache.commons.dbcp.DelegatingPreparedStatement.executeUpdate
   (DelegatingPreparedStatement.java:207)
at com.brightmail.dl.jdbc.impl.DatabaseSQLManager.handleUpdate(Unknown Source)
at com.brightmail.dl.jdbc.impl.DatabaseSQLManager.handleUpdate(Unknown Source)
at com.brightmail.dl.jdbc.impl.DatabaseSQLTransaction.create(Unknown Source)
at com.brightmail.bl.bo.impl.SpamManager.create(Unknown Source)
at com.brightmail.service.smtp.impl.SmtpConsumer.run(Unknown Source)
```

Users Don't See Distribution List Messages in Their Quarantine

When Brightmail AntiSpam forwards a spam message sent to a distribution list to Quarantine, the message is not delivered in the intended recipients' quarantine. Instead, the message is delivered to a special Quarantine mailbox for that distribution list. For more information, see "Notification for Distribution Lists/Aliases," on page 102.

Undeliverable Quarantined Messages Go to Quarantine Postmaster Mailbox

If Quarantine can't determine the proper recipient for a message received from Brightmail AntiSpam, it delivers the message to a `postmaster` mailbox accessible from Quarantine. Your network may also have a `postmaster` mailbox you access using a mail client that is separate from the Quarantine `postmaster` mailbox. To display messages sent to the Quarantine `postmaster` mailbox, see "Checking the Quarantine Postmaster Mailbox," on page 111.

Error in Quarantine Log File Due to Running Out of Disk Space or Full Work Directory

If you check Quarantine log file as described in "Checking the Quarantine Error Log," on page 112 and see lines similar to those listed below, make sure that you haven't run out of disk space on the computer where Quarantine is installed. If that isn't the problem, follow the steps below.

```
9 Jan 2004 00:00:22 (ERROR:5396:6396):[2032] Error connecting to
   192.168.1.4:41025: Unknown Error; Out of range.
9 Jan 2004 00:00:22 (ERROR:5396:6396):[4042] smtp_direct: failed to connect to
   SMTP server.
9 Jan 2004 00:00:22 (ERROR:5396:6396):[4019] Module SMTP_DIRECT failed on
   message C:\Program Files\Brightmail\bmispool\1184.1072896064.9305:processing
   halted.
```

1 Delete the following directory:

```
UNIX:
.../Tomcat/jakarta-tomcat-version/work
Windows:
...\Tomcat\jakarta-tomcat-version\work
```

2 Reboot the computer where Quarantine is installed.

3 Make sure the following directory is empty:

```
UNIX:
/opt/brightmail/bmispool
Windows:
C:\Program Files\Brightmail\bmispool
```

Users Receive Notification Messages, but Can't Access Messages in Quarantine

If some users at your company can successfully log into Quarantine and read their spam messages, but others get a message saying that there are no messages to display after logging in to Quarantine, there may be a problem with the Active Directory (LDAP) configuration. If the users who can't access their messages are in a different Active Directory domain than the users who can access their messages, configure LDAP in the Brightmail Control Center to use a Global Catalog, port 3268, and verify that the nCName attribute is replicated to the Global Catalog as described in "Configuring a Global Catalog to Work With Quarantine," on page 82.

Duplicate Messages Appear in Quarantine When Logged in as Administrator

You may notice multiple copies of the same message when logged into Quarantine as an administrator. When you read one of the messages, all of them are marked as read. This behavior is intentional. If a message is addressed to multiple users at your company, Quarantine stores one copy of the message in its database, although the status (read,

deleted, etc.) of each user's message is stored per-user. Because the administrator views all users' messages, the administrator sees every user's copy of the message. If the administrator clicks on **This is not Spam**, just the selected message or messages are redelivered to the users' mailboxes, not all the duplicate messages.

Maximum Number of Messages in Quarantine

If you don't set any Quarantine thresholds and your system has adequate capacity, there is a 1 TB (terabyte) MySQL limit on the number of messages that can be stored in Quarantine (the same message sent to multiple recipients counts as one message). For more information about Quarantine thresholds, see "Specifying Quarantine Message and Size Thresholds," on page 109.

Copies of Misidentified Messages Aren't Delivered to Administrator

If you typed an email address in the **Administrator** box under **Misidentified Messages** on the **Quarantine Settings** page but messages aren't being delivered to the email address, make sure the email address is not an email alias. The administrator email address for misidentified messages must be a primary email address including the domain name, such as `admin@example.com`.

Search Results aren't as Expected

Because it is optimized to produce relevant matches from a large number of messages, searching messages in Quarantine sometimes yields unexpected results. For example, if any term in the search phrase matches 50% or more of the messages in the database, then the search will show no results. This behavior may be particularly noticeable if you have a very small number of messages in Quarantine. See "Search Details," on page 95 for more information about Quarantine search behavior.

Monitoring Symantec Brightmail AntiSpam

Getting System Status

The **Summary** tab lets you:

- View at a glance how Symantec Brightmail AntiSpam is performing.
- View the graphs for recent spam and virus filtering statistics.
- View summary status about filters and enabled components.

The following table shows what is available from the summary tab.

Table 19. Items Available on Summary Tab

Item	Summarizes	Available Operations
System Status	• Whether antivirus or antispam filtering is enabled or disabled • Whether Brightmail Servers are accessible • Whether filters are current. Filters are considered "out of date" if an update has not been received in the time frame specified in the **Alerts** page on the **Setting** tab. • Quarantine disk space usage	If available, click the links in the rightmost column to go to the **Status** tab for more information.
Last 60 Minutes	Message processing and filtering over the last 60 minutes.	Display only.
Totals Since date	Message processing and filtering statistics since a point in time.	Click **Reset** to clear the values and start a new point in time.
Last 24 Hours	Message processing and filtering over the last 24 hours	Use the **Display** list to choose whether to chart percentages of caught spam, viruses, or both.
Last 30 Days	Message processing and filtering over the last 30 days	Use the **Display** list to choose whether to chart percentages of caught spam, viruses, or both.

Working with Logs

Each Brightmail Scanner maintains a database of log information. Viewing these logs in the Brightmail Control Center can help you diagnose error conditions and keep track of many aspects of your system during its operation.

You can choose to store logging data for the following components:

- Brightmail Server
- Brightmail Client
- Conduit
- Harvester
- AntiVirus Cleaner

You can designate the severity of errors you want written to the log files. Brightmail AntiSpam provides five logging levels, with each successive level including all errors from the previous levels. The default logging level for each Brightmail software component is “Warnings.” Your choices, from the least to the greatest amount of error reporting, are:

- Errors
- Warnings
- Notices
- Information
- Debug

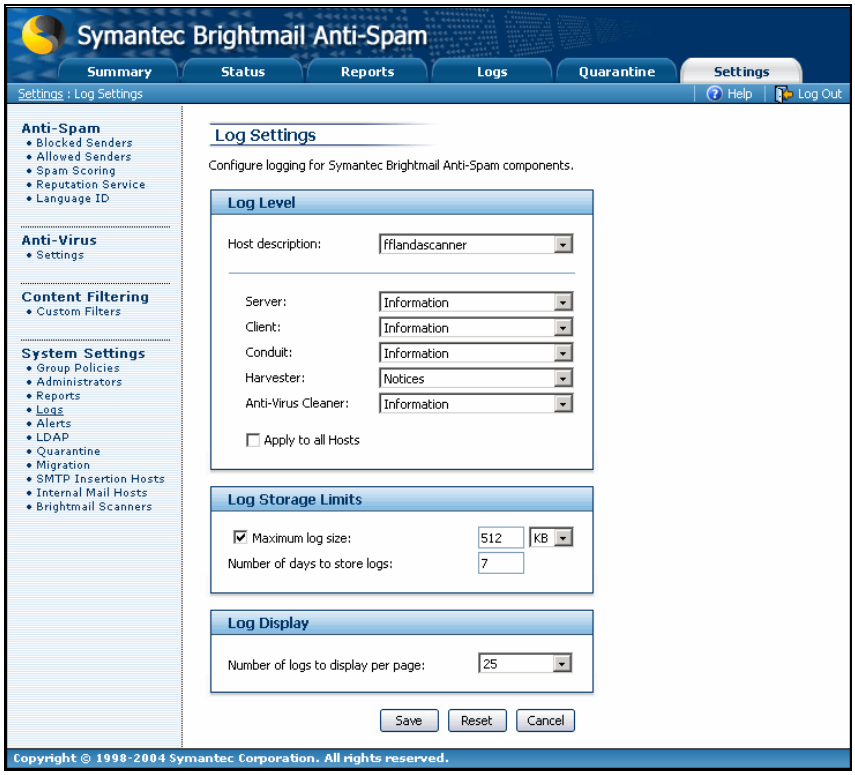
To limit the size of the database that stores log data on Brightmail Scanner machines, Brightmail AntiSpam stores seven days of log data, with a maximum storage allotment of 512 MB. If the database already has 512 MB of data or seven days of data, the oldest log data will be deleted as new log data comes into the system. To keep more log data for a longer period, you can change the default maximum log size and retention period settings.

Modifying Log Settings

To modify log settings for a Brightmail Scanner:

1. In the Brightmail Control Center, click the **Settings** tab.
2. In the left pane, under **System,** click **Logs**.

   The Log Settings page is displayed.



3 Use the **Host description** list to specify the Brightmail Scanner for which to adjust log settings.

4 For each component listed, select a log level, corresponding to the severity of errors you want written to the log file.

5 If desired, select **Apply to all hosts** to apply the same log level settings to all hosts.

6 In the **Log Storage Limits** section, do any of the following to keep the size of logs manageable:

— To restrict the size of the database that stores log data, click **Maximum log size** and then specify a size using the box and arrow.

— To restrict the number of days for which Brightmail AntiSpam logs data, complete the **Number of days to store logs** box.

7 To increase or decrease the number of logs entries to display on the **Logs** tab, enter a new value in the **Number of logs to display per page** box.

8 Click **Save**.

For changes to log file locations to take effect, you must restart the selected component. Click **OK** to save your settings and restart the component; click **Cancel** to save your settings without restarting the component.

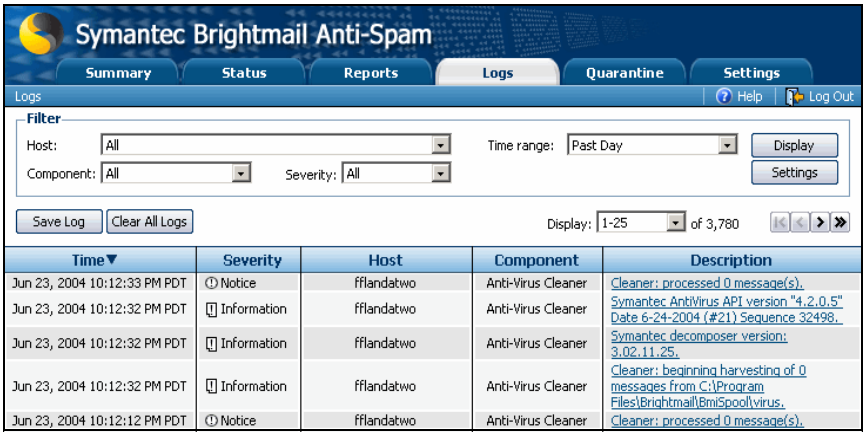
Viewing and Saving Logs

You can view logs for a specific Brightmail Scanner or you can view logs for all Brightmail Scanners. You can also choose to save logs to a text file for further review and editing with another application.

To view logs for a Brightmail Scanner:

1 In the Brightmail Control Center, click the **Logs** tab.

The Logs page is displayed.



2 In the **Filter** section, do the following**:**

a. Use the **Host** list to specify the Brightmail Scanner you want to work. Select **All** to view log data for all configured Brightmail Scanners.

b. Use the **Component** list to select the specific component for which you want to view log information. Select **All** to view log data for all components.

c. In the **Time range** list, do one of the following:

- To specify a preset range, select **Past Hour**, **Past Day**, **Past Week**, and **Past Month**.
- To specify a different time period, select **Customize** and then click the calendar icons to the right of the **Start Date** and **End Date** to graphically select a time range.

d. Use the **Severity** list to select the type of errors you want to view.

3 Click **Display**.

The **Logs** tab updates to show logs entries based on the filter you created. Log entries are presented in summary form as rows in a table. Click the **Description** link for an entry to jump to a detailed view.

4 After the logs have loaded in the browser, you can do one of the following:

— To save the log information for the current query to a text file for further review, click **Save Log** and then click **Save** in the next dialog box.

— To remove *all* stored log data, click **Clear All Logs** and then click **OK** to dismiss the confirmation message.

— To adjust settings for Brightmail logs, such as the number of entries to display on a page or the logging levels, click **Settings**.

Setting Up Event-Based Alerts

When certain operating conditions arise, Brightmail AntiSpam automatically sends email alerts to administrators. The conditions that generate alerts are the following:

- A Brightmail component is not responding or working.
- Antispam filters are older than a specified time.
- Antivirus filters are older than a specified time.
- Disk space is low.

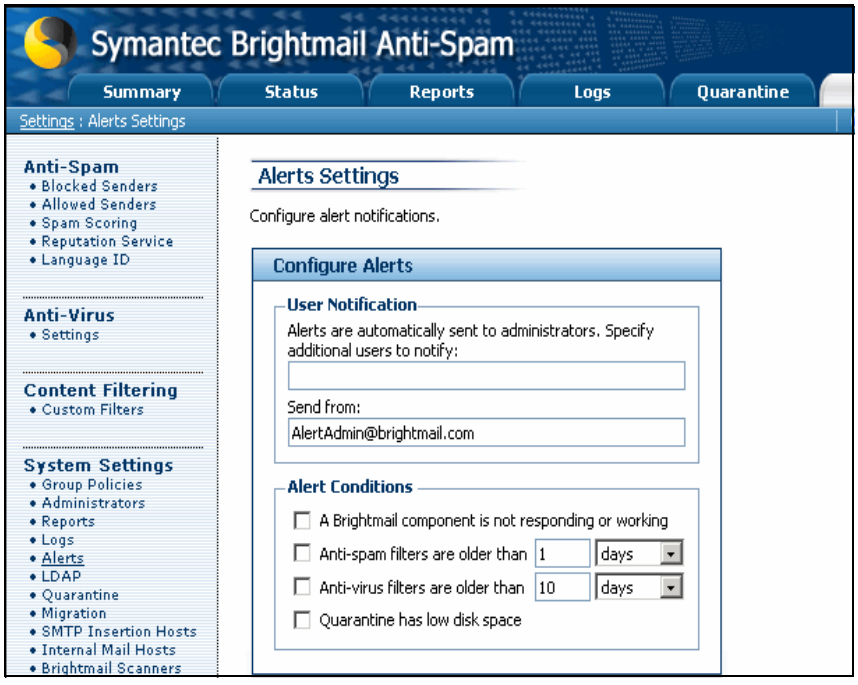
The **Alerts** page lets you specify when filters will be considered out of date. Brightmail AntiSpam consults these settings when displaying the filter status on the **Summary** and **Status** tabs. You can also specify a list who will be informed via email when alert conditions arise.

To set up alerts:

1 In the Brightmail Control Center, click the **Settings** tab.

2 In the left pane, under **System Settings**, click **Alerts**.

The Alerts Settings page is displayed.



3 Under **User Notification**, specify a list of email addresses of users who should receive alerts. Separate multiple email addresses with commas.

4 In the **Send from** box, type the email address that the alert should appear to be from.

5 Under **Alert Conditions**, click the check box next to the condition for which you want to send alerts.

6 If you want be notified when filters are out of date, complete the necessary date boxes.

To avoid receiving unnecessary alerts, do not set the **AntiSpam filters are older than** setting to less than 2 hours. While most antispam filters are disseminated every 5 to 10 minutes, Brightmail Reputation Service filters are updated every hour or so. Also note that antivirus filters are not propagated as frequently as AntiSpam filters and are initiated by Symantec, not Brightmail.

7 Click **Save**.

Periodic System Maintenance

System maintenance of the Brightmail software should be done as part of your regular server maintenance schedule, including the tasks below.

Backing Up MySQL Data

There are four types of data that Brightmail AntiSpam stores in the MySQL database:

- Configuration data for your system
- Logs
- Reports
- Brightmail Quarantine messages (only exists if you are using Brightmail Quarantine)

You can back up these data types together or separately, using MySQL. If you have a large number of messages in your Quarantine, backing up Quarantine may take some time.

Backups can be done while the Brightmail software is running. MySQL must be running when you perform backups.

For complete instructions on performing backups of MySQL data, see the MySQL documentation. The following MySQL commands are suggested for your use.

To determine your current MySQL Password:

1. Open a console window (Solaris/Linux) or Command Prompt (Windows) as an administrator.
2. Locate your Tomcat installation directory by running the appropriate command:

   Linux/Solaris:

```
grep "CATALINA_HOME=" /etc/init.d/tomcat4
```

Windows:

```
set CATALINA_HOME
```

3. Open the file `$CATALINA_HOME/conf/server.xml` (UNIX) or `$CATALINA_HOME\conf\server.xml` (Windows) with a text editor. On UNIX, open the file while logged in as root.
4. Locate the following section under the `/brightmail` Context.

```
<!-- MySQL dB username and password for dB connections  -->
   <parameter>
<name>username</name>
<value>brightmailuser</value>
</parameter>
<parameter>
<name>password</name>
<value>password</value>
</parameter>
```

5. Note the current password in `<value>password</value>`.
6. Exit from the `server.xml` file.

Backing Up Configuration Data Only

To save the configuration tables:

```
mysqldump --user=brightmailuser --password=PASSWORD --opt brightmail admin_user
   black_white_sender host settings_alert settings_consent settings_ldap
   settings_log settings_quarantine settings_report settings_scheduled_reports
   settings_smtp_filter_host settings_smtp_mngnt_host settings_system
   sieve_condition sieve_import sieve_rule status status_rule --host=127.0.0.1
   > configuration.sql
```

To restore configuration tables from backup:

```
mysql --user=brightmailuser --password=PASSWORD brightmail --host=127.0.0.1 <
   configuration.sql
```

Backing Up Reports Data Only

To save the Reports tables:

```
mysqldump --user=brightmailuser --password=PASSWORD --opt brightmail
   report_alias report_domain report_ip_address report_summary settings_report
   settings_scheduled_reports --host=127.0.0.1 > report.sql
```

Backing Up Reports Data Only

To restore the Reports tables from backup:

```
mysql --user=brightmailuser --password=PASSWORD brightmail --host=127.0.0.1 <
   report.sql
```

Backing Up Logs Data Only

In general, there is no reason to store stale logs. For troubleshooting purposes, logs that are not set to `Information` (which provides the most detail) have limited utility, especially if you need assistance from Brightmail Support personnel. It is best to view and save current logs as needed on the **Logs** tab and set the appropriate retention period for logging data. If you choose to back up files in the `logs` database stored on the Brightmail Control Center, you can use the following `mysqldump` commands.

To save the Logs tables:

```
mysqldump --user=brightmailuser --password=PASSWORD --opt brightmail log
   log_component log_marker log_severity log_summary settings_log
   --host=127.0.0.1 > log.sql
```

To restore the Logs tables from backup:

```
mysql --user=brightmailuser --password=PASSWORD brightmail --host=127.0.0.1 <
   log.sql
```

Backing Up Quarantine Data Only

To save Quarantine tables:

```
mysqldump --user=brightmailuser --password=PASSWORD --opt brightmail user
   user_spam_message spam_message spam_message_summary
   spam_message_release_audit settings_quarantine settings_ldap
   --host=127.0.0.1 > quarantine.sql
```

To restore Quarantine tables from backup:

```
mysql --user=brightmailuser --password=PASSWORD brightmail --host=127.0.0.1 <
   quarantine.sql
```

Backing Up All Brightmail Data Simultaneously

To save the Brightmail database:

```
mysqldump --user=brightmailuser --password=PASSWORD --opt brightmail
   --host=127.0.0.1 > brightmail.sql
```

To restore the Brightmail database from backup:

```
mysql --user=brightmailuser --password=PASSWORD brightmail --host=127.0.0.1 <
   brightmail.sql
```

Maintaining Adequate Disk Space

Use standard file system monitoring tools to verify that you have adequate disk space. Remember that the storage required by certain Brightmail features, such as extended reporting data and Quarantine can become large.

Checking the Status of the MySQL Database

If you encounter problems logging into Brightmail Control Center or Quarantine, you may wish to check the status of your MySQL database, especially if the hardware the MySQL database is running on was improperly shut down. The `brightmail_check_db` scripts will run `mysqlcheck` to repair tables if necessary.

- On UNIX, `brightmail_check_db.sh` is in
  `USER_INSTALL_DIR/MySQL/mysql*/scripts`
- On Windows, `brightmail_check_db.bat` is in
  `MYQSL_INSTALL_DIR\scripts`

To run the scripts:

- On UNIX:

```
% cd USER_INSTALL_DIR/MySQL/mysql*/scripts
% ./brightmail_check_db.sh
```

- On Windows:

Open a DOS command window.

```
cd MYSQL_INSTALL_DIR\scripts
brightmail_check_db.bat
```

Degraded Effectiveness Due to Expired License

Symantec Brightmail AntiSpam must have a current license to operate. If your license is expired you will not be able to receive filter updates, and the effectiveness of your protection will rapidly degrade. If you upgraded your installation from an initial Version 6.0 or earlier installation, the Brightmail Control Center Status page will not warn you of license expiration. Regardless of version, log messages will warn you when your license has expired. To purchase a new license, contact your Symantec sales person or go to the following URL:

http://www.symantecstore.com/renew

Checking Versions

To check the versions of your installed software, go to:

`http://prefix.yourcompany.com:port/brightmail/BrightmailVersion`

where *`port`* is the port that Tomcat uses.

You can see the installed versions of the following software:

- Brightmail Control Center

- Brightmail Quarantine
- Java
- MySQL

Appendix A: Creating Filters by Coding in Sieve

If you are familiar with the Sieve language, you can create custom filters by directly editing a Sieve filters file instead of using the Custom Filters Editor.

Symantec Brightmail AntiSpam provides an implementation Sieve. The Sieve filters file you create must adhere to this implementation: for Unix and for Windows. This section describes the differences between the RFC3028 version of Sieve and the Brightmail implementation of Sieve

This section assumes a thorough understanding of all Sieve commands, particularly those not included here. For a generalized description of Sieve, visit the site `http://www.faqs.org/rfcs/rfc3028.html`. In particular, see descriptions of the `require` and `header` control commands.

Working with the Manually Edited Sieve Filters File

The following general guidelines can be useful as you write Sieve scripts.

Restart the Brightmail Server After Editing the Sieve Script

Whenever you manually edit the Sieve filters file, you need to restart all the Brightmail Servers for the new Sieve filters to take effect. The easiest way to do this is to click the **Status** tab in the Brightmail Control Center, select all enabled Brightmail Servers, click **Stop**, and then click **Start**. See "Starting and Stopping Symantec Brightmail AntiSpam," on page 31 for more information.

Using the Custom Filters Editor Erases Changes to Sieve Filters File

Although you can manually edit the Sieve code created by the Custom Filters Editor, as soon as you add another filter using the Custom Filters Editor, your manual changes will be overwritten.

Avoid Nesting If-Then Statements

Deeply nested if-then statements may result in impaired performance. Consider writing long sequences of separate if-then statements instead.

Pay Attention to White Space

Multiple white spaces in an email header or body are treated as a single `space` character (ASCII 0x20). For example, “ `foo`” is treated as “ `foo`”.

Terminate Execution Promptly

In general, you should terminate execution as early in the script as possible, using `stop` statements immediately after an action is specified, for instance.

You might also structure scripts so that conditions with the highest probability of script matching appear first. For instance, if all messages from `example.net` will trigger the `matched` action, and if most of your messages come from `example.net`, then test for `example.net` early in the script.

The `body` test is the most CPU-intensive, so you may want to add it as the last test in a sequence, so that other, less intensive tests may trigger first.

Remember That Encoded Headers are Not Decoded Before Being Tested

Headers that contain text using RFC2047 encodings are tested based on their encoded values. Note that mail clients would display the decoded values of these headers.

Sieve Implementation Details

Sieve Filters File Location

Upon initialization, Brightmail Servers attempt to retrieve Sieve filters stored in the file `sieve_script.txt`, located in the following directories:

- Windows: `C:\Program Files\Brightmail\Config`
- Unix: `/opt/brightmail/`

You can review a sample file of Sieve filters in the `etc` subfolder.

- Windows: `C:\Program Files\Brightmail\etc\sieve_script.sample.txt`
- Unix: `/opt/brightmail/etc/sieve_script.sample`

To begin using Sieve scripts, copy the sample file to the file named `sieve_script.txt`.

After you make changes to custom filters in this file, follow the procedures in “Importing a Custom Filters File,” on page 64.

Supported Sieve Commands

The Sieve language contains three types of commands:

- Control
- Action
- Test

Brightmail supports the Control commands described in http://www.faqs.org/rfcs/rfc3028.html. The following sections provide you with documentation on the Action and Test commands in the Brightmail implementation of Sieve.

Only the `keep` and `matched` (equivalent to `sideline`) action commands should be used in the Brightmail implementation of Sieve for Windows. None of the other action commands described in RFC3028 should be used in your Sieve scripts. For example, instead of using the `discard` action command, in your group policies, set the action to take for **Company-specific Content** (messages that match custom filters) as **Delete the message**. You can view or change the setting as follows:

1. In the **Brightmail Control Center**, click the **Settings** tab.
2. In the left pane, under **System Settings**, click **Group Policies**.
3. Choose the group policy you want to edit by clicking on the underlined group policy name.
4. Scroll down to the **Company-specific content** section.
5. Click on the drop-down menu and choose the action you want.
6. Click **Save**.

Sieve Action Commands

The Brightmail implementation of Sieve supports the following Action Commands:

Keep

The `keep` command files a message into the user's inbox. If a message does not match any filters in your Sieve script, that message has an effective action of `keep` and is delivered to the user's inbox.

Matched

The `matched` command indicates that a test condition has been met regarding the message being processed. The `matched` command is a Brightmail extension to the standard set of Sieve Action commands.

When a match occurs, the message is handled using the action specified for **Company-specific Content** on the **Group Policies** settings page in the Brightmail Control Center, for the group policy that applies to the recipient.

The capability string to specify for the `matched` command with `require` is `sideline`.

```
Syntax:  matched
```

Example

```
require "sideline";
if allof (header :is "to" "eric@pku.edu.cn",
          header :is "subject" "job opening")
```

```
{
   matched;
   stop;
}
```

When a match occurs, the message is handled using the action specified for **Company-specific Content** on the **Group Policies** settings page in the Brightmail Control Center, for the group policy that applies to the recipient. In this example, all messages sent to `eric@pku.edu.cn` with the words `job opening` as the subject line will be processed based on the action specified for **Company-specific Content** for the group policy that applies to the recipient of the email (in this case, this will be `eric@pku.edu.cn`)

Sieve Test Commands

The Brightmail implementation for Windows of Sieve includes standard, modified, and new test commands. The following standard Sieve test commands are supported by the Brightmail software, and behave as documented in RFC3028:

- `address` — Tests for the presence of specific email addresses in header lines (your system's performance may degrade if you search for a long list of email addresses)
- `allof` — Performs a logical AND on the tests supplied to it
- `anyof` — Performs a logical OR on the tests supplied to it
- `exists` — Tests for the presence of the specified header(s)
- `false` — Always evaluates to false
- `header` — Tests for the presence of a character string in the specified header (does not apply to MIME entity headers). Headers are defined in `http://www.faqs.org/rfcs/rfc2822.html`.
- `not` — Takes another test as an argument, and yields the opposite result
- `size` — Tests if a message is over or under the specified size
- `true` — Always evaluates to true

The following Sieve test commands have been modified or are new extensions implemented by Brightmail, and are explained below:

- `body` — This Brightmail test command searches the body of a message for a string.
- `envelope` — Tests for specified email addresses in the SMTP envelope as described in RFC3028. The Brightmail implementation also allows you to test for the `HELO`/`EHLO` domain and the IP address of the machine contacting the server.
- `mimeheader` — This Brightmail test command searches both normal and MIME headers for a string.

Body

The `body` test evaluates to true if any line of the body of a message contains any listed key, however it does not examine MIME headers. The body test will examine text MIME

attachments, but not binary MIME attachments (even if they contain text, such as Microsoft Word `.doc` files).

NOTE: *RFC2822 defines what constitutes the body of an email message. Basically, all text that follows the CR/LF lines that end the header section is the body. See* `http://www.faqs.org/rfcs/rfc2822.html` *for details.*

The capability string to specify for the `body` test with `require` is `body`.

```
Syntax:  body <comparator> [MATCH-TYPE] <key-list: string>
```

Example

```
require ["body", "sideline"];
if body :contains "top-secret"
{
   matched;
   stop;
}
```

This example tests for `top-secret` in the body of the message. If found, the message is handled using the action specified for **Company-specific Content** on the **Group Policies** settings page in the Brightmail Control Center, for the group policy that applies to the recipient.

Envelope

As described in RFC3028, you can use `from` to search the FROM address used in the SMTP MAIL command, and `to` to search the TO address used in the SMTP RCPT command. In addition, Brightmail provides extensions to the `envelope` command as follows:

- `Helo` — Tests the sending domain listed in the `HELO`/`EHLO` SMTP command stored in the envelope.
- `peerip` — Tests the IP address of the SMTP client that has contacted the local MTA. The `i;ip-mask` comparator supports match types `:is` and `:contains`. Notations supported for comparison are:
  - Single host: 128.113.213.4
  - Netmask Source-IP: 128.113.1.0/255.255.255.0
  - CIDR: 198.0.0.0/8 (equivalent to 198.0.0.0/255.0.0.0)

The capability string to specify for the `envelope` test with `require` is `envelope`.

```
Syntax: envelope <comparator> [MATCH-TYPE] <key-list: string>
```

Unless the Brightmail software is in communication with an MTA that is deployed at the border of the Internet (your gateway), the envelope domain or IP address on a message checked by the envelope test may be the internal domain that passed on the message from the email gateway, rather than the Internet address you might expect.

The envelope information is not usually visible in mail reading programs like Outlook.

Mimeheader

The `mimeheader` test searches for all headers at the beginning of the messages as well as MIME headers. This test is particularly helpful in identifying messages containing executable MIME attachments. It is syntactically identical to the `header` test.

The capability string to specify for the `mimeheader` test with `require` is `mimeheader`.

```
Syntax:  mimeheader <comparator> [MATCH-TYPE]
             <header-names: string> <key-list: string>
```

Example

```
require ["mimeheader", "sideline"];
if mimeheader :contains "Content-Type" ".jpg.vbs"
{
   matched;
   stop;
}
```

In this example, if *any* MIME header `Content-Type` contains the substring `.jpg.vbs` (a Visual Basic script renamed to appear to be an image file). If found, the message is handled using the action specified for **Company-specific Content** on the **Group Policies** settings page in the Brightmail Control Center, for the group policy that applies to the recipient.

Example

```
require ["mimeheader", "sideline"];
if anyof
   (mimeheader :contains "Content-Disposition"
        "filename=AnnaKournikova.jpg.vbs",
    mimeheader :contains "Content-Type"
         "name=AnnaKournikova.jpg.vbs")
{
   matched;
   stop;
}
```

In this example, the filename is checked for both the `Content-Disposition` and `Content-Type` headers. If the target filename appears in either header type, the message is handled using the action specified for **Company-specific Content** on the **Group Policies** settings page in the Brightmail Control Center, for the group policy that applies to the recipient.

Example

```
require ["mimeheader", "sideline"];
if mimeheader :contains "Content-Type" ["video", "audio"]
{
   matched;
   stop;
}
```

In this example, the system will handle messages containing `video` or `audio` type attachments using the action specified for **Company-specific Content** on the **Group Policies** settings page in the Brightmail Control Center, for the group policy that applies to the recipient. Note that MIME types do not have to reflect the actual contents. A video or audio attachment could be sent as `application/octet-stream`.

Successful blocking of unwanted content will require the analysis of both filenames and media types in many cases.

Sieve Action Precedence

When a Sieve script runs, multiple actions can be combined. However, only the action with the highest precedence will be applied to the message. When combined, the two supported Sieve actions, in order of precedence, behave as follows:

- `matched` — If the execution of a script results in both `matched` and `keep`, the `keep` will be ignored.
- `keep` — If the execution of the script results in no actions, a `keep` will be performed.

NOTE: `custom_*` *takes precedence over matched and keep. Only one* `custom_*` *Sieve action can be returned at a time.*

Sample Sieve Scripts

Following are examples of Sieve scripts used for a variety of tasks. The action taken on matching messages depends on the policies you have in place for content filters.

Intercept adult content

This example catches potentially offensive content.

A longer version of this sample Sieve script is in the following locations:

- Windows: `C:\Program Files\Brightmail\etc\sieve_adult.txt`
- Unix: `/opt/brightmail/etc/sieve_adult.sample`

A sample email message you can send through your email server to test this script can be found here:

- Windows: `C:\Program Files\Brightmail\etc\tests\sieve.adult.msg`
- Unix: `/opt/brightmail/etc/tests\sieve.adult.msg`

NOTE: Both files contain obscene language.

```
#
# filter adult content
#
require ["body", "sideline"];

# filter based on sender
if header :contains "from" "porn king"
```

```
{
   matched;
   stop;
}

# filter based on subject
if header :contains "subject" "hot pics"
{
   matched;
   stop;
}
if header :contains "subject" "adults only"
{
   matched;
   stop;
}
# filter using wildcards
if body :matches "*mailto*@btamail.net*"
{
   matched;
   stop;
}

# filter based on domain names and URLs
if body :contains "worldwidewebhost"
{
   matched;
   stop;
}
if body :contains "www.netmails.com/members"
{
   matched;
   stop;
}

# filter based on body text
if body :contains "hot girls"
{
   matched;
   stop;
}

# look for combination of suspicious words in subject header
if allof (
anyof (
header :contains "subject" " hot",
header :contains "subject" "sexy"
),
anyof (
header :contains "subject" "girls",
header :contains "subject" "women"
))
```

```
{
   matched;
   stop;
}
```

Set a size limit on incoming mail

This example sets a match for any email message larger than one megabyte.

```
require "sideline";
   if size :over 1M
{
   matched;
   stop;
}
```

Intercept chain letters

This example catches a particular chain letter.

```
# catch chain letters
require "sideline";
if anyof (header :is "Subject"  "DO NOT DELETE!! THIS REALLY WORKS!!!!",
   header :is "Subject" "RE: DO NOT DELETE!! THIS REALLY WORKS!!!!")
{
   matched;
   stop;
}
```

Intercept a particular virus

This example catches the `Anna Kournikova` virus.

```
# catch the kournikova virus
require ["mimeheader", "sideline"];
if anyof
   (mimeheader :contains "Content-Disposition"
        "filename=AnnaKournikova.jpg.vbs",
    mimeheader :contains "Content-Type"
         "name=AnnaKournikova.jpg.vbs")
{
    matched;
    stop;
}
```

Intercept greeting cards

This example catches messages from the domain `bmarts.com`, a source of greeting cards.

```
# catch greeting cards
require "sideline";
if header :contains "Received" "bmarts.com"
{
    matched;
    stop;
}
```

Intercept senders based on the HELO domain

You can create custom filters to test based on the results of the `HELO domain` API call. The `HELO`/`EHLO` domain is available via the envelope `helo` data.

```
require ["envelope", "sideline"];
if envelope :matches "helo" "spammer.com"
{
   matched;
   stop;
}
```

Appendix B: Editing Virus Notification Messages

Whenever the Symantec Brightmail AntiSpam sidelines and processes a message for virus cleaning, it extracts the appropriate text from an XML file and creates an advisory message that informs the recipient of the action taken. Symantec Brightmail AntiSpam then inserts the original message as an attachment to the advisory message. This method ensures that the advisory message is always presented to the user, and that the original message is included unless it has been deleted as uncleanable.

Although it is not necessary for you to edit these messages, you can do so if you wish. This section explains the format of the file that contains the messages and the procedure for modifying it.

Customizing the Cleaner Notification File

You can edit the file, `Notification.xml`, to customize advisory text that Brightmail AntiSpam uses. The file is located at:

- `C:\Program Files\Brightmail\etc\Notification.xml` (Windows)
- `/opt/etc/brightmail/Notification.xml` (Unix)

At the beginning of `Notification.xml`, it is possible to change the character set and content transfer encoding to be used for the advisory messages. By default, Brightmail software uses the `US-ASCII` character set and `7 bit` encoding to send the advisory text in the XML notification template. `Notification.xml` includes two tags, `<char-set>` and `<content-transfer-encoding>`. You can edit these tags to specify a different character set or content encoding for AntiVirus Cleaner notification messages.

For example, to use the `Latin 2` character set `(ISO 8859-2)`, which contains characters for 15 Eastern European languages, you would edit these two tags to appear as follows:

```
<char-set>"ISO-8859-2"</char-set>
<content-transfer-encoding>"8bit"</content-transfer-encoding>
```

For a list of all the languages that use the `ISO 8859` character sets, see: http://www.czyborra.com/charsets/iso8859.html.

In addition, you may want to provide more or less detail in these notifications, depending on your audience. In the XML file, each notification message is constructed with an **`<advisory>`** element. There are several **`<advisory>`** elements, each containing a block of information, depending on the disposition of the message.

For example, after Brightmail AntiSpam successfully cleans a message, it retrieves text from the **cleaned_sentence** advisory, shown in the following excerpt from the XML file:

```
<advisory name="cleaned_sentence">

<text><t name="file_name"/> was infected with the malicious virus
   <t name="virus_name"/> and has been cleaned.</text>

</advisory>
```

Caution

When making changes to the XML file, modify only customizable text. If you adjust the placement of the variable tags identified by the `<t>` ***tag, ensure that you don't change the values of the tokens within the tag. Do not modify any other tags or structures****.*

For example, to make changes to the text Brightmail AntiSpam inserts for cleaned messages, only edit the **`boldface`** *text, as shown in the following example:*

```
<advisory name="cleaned_sentence">

<text><t name="file_name"/> was infected with the malicious virus
   <t name="virus_name"/> and has been cleaned.</text>

</advisory>
```

To view all customizable `<advisory>` elements in `Notification.xml`, see the next section.

Cleaner Notification File Listing

This section shows the full contents of the Cleaner Notification file, `Notification.xml`, which contains text for notifications issued by the Cleaner as it sidelines and processes messages. You can modify certain text in `<advisory>` elements, as described in the previous section.

```
<?xml version=”1.0” encoding=”iso-8859-1”?>
<!DOCTYPE advisory-list  SYSTEM “AdvisoryStore.dtd”>

<!-- @version: -->

<advisory-list char-set=”us-ascii” content-transfer-encoding=”7bit”>

<!-- The following eleven notifications are the new v2 notification
     scheme.  -->

<advisory name=”cleaned_sentence”>
<text><t name=”file_name”/> was infected with the malicious virus <t
   name=”virus_name”/> and has been cleaned.</text>
</advisory>

<advisory name=”deleted_cant_clean_sentence”>
<text><t name=”file_name”/> was infected with the malicious virus <t
   name=”virus_name”/> and has been deleted because the file cannot be
   cleaned.</text>
</advisory>

<advisory name=”deleted_cant_replace_sentence”>
<text><t name=”file_name”/> was infected with the malicious virus <t
   name=”virus_name”/> and has been deleted because the Symantec decomposer
   cannot modify its container.</text>
</advisory>

<advisory name=”deleted_too_large_sentence”>
<text><t name=”file_name”/> was deleted because it is too large.</text>
</advisory>

<advisory name=”deleted_cant_rebuild_sentence”>
<text><t name=”file_name”/> was deleted because the Symantec decomposer
   cannot rebuild its container.</text>
</advisory>

<advisory name=”virus_still_there_sentence”>
<text><t name=”file_name”/> is still infected with the malicious virus <t
   name=”virus_name”/> because the Symantec decomposer cannot modify its
   container.</text>
</advisory>

<advisory name=”cant_scan_container_corrupted_sentence”>
```

```
<text>The container <t name=”file_name”/> was not scanned because it is
   corrupted (Symantec decomposer reports <t name=”error”/>). If you are able
   to open it, use caution when doing so as it may contain files with
   viruses.</text>
</advisory>

<advisory name=”cant_scan_oless_corrupted_sentence”>
<text>The Microsoft document <t name=”file_name”/> was not scanned because it
   is corrupted (Symantec decomposer reports <t name=”error”/>). If you are
   able to open it, use caution when doing so as it may contain embedded
   files with viruses.</text>
</advisory>

<advisory name=”cant_scan_encrypted_sentence”>
<text><t name=”file_name”/> was not scanned for viruses because it is
   encrypted.</text>
</advisory>

<advisory name=”cant_scan_too_large_sentence”>
<text><t name=”file_name”/> was not scanned for viruses because it is too
   large.</text>
</advisory>

<advisory name=”scan_error_sentence”>
<text><t name=”file_name”/> was not scanned for viruses because of the error:
   <t name=”error”/></text>
</advisory>


<!-- The following two notification sentences are for the old v1
     notification scheme.  We have replaced it with the newer v2
     notification scheme because the notices are more granular.
     NOTE: cleaned_sentence is still used in v2, so it is not included
     here. -->

<advisory name=”deleted_sentence”>
<text><t name=”file_name”/> was infected with the malicious virus <t
   name=”virus_name”/>, but was unable to be cleaned, and has been removed.</
   text>
</advisory>

<advisory name=”error_sentence”>
<text><t name=”file_name”/> is believed to be infected, but the condition
   cannot be confirmed, or the file cannot be disinfected.  It is recommended
   that you DO NOT open the file without first checking with your system
   administrator and/or the sender.</text>
</advisory>


<advisory name=”rcpt_text”>
<text>This message has been processed by Brightmail(r) AntiVirus using
Symantec’s AntiVirus Technology.

<t name=”file_actions”/>
```

```
For more information on antivirus tips and technology, visit
http://www.brightmail.com/antivirus .
</text>
</advisory>


<advisory name=”rcpt_html”>
<text>
<![CDATA[
<HTML>
<BODY>
<P>
This message has been processed by Brightmail&#174; AntiVirus using<BR>
Symantec’s AntiVirus Technology.<BR>
<BR>
<PRE>
]]>
<t name=”file_actions”/>
<![CDATA[
</PRE>
<BR>
For more information on antivirus tips and technology, visit
<A HREF=”http://www.brightmail.com/antivirus”>
http://www.brightmail.com/antivirus</A>.
</P>
</BODY>
</HTML>
]]>
</text>
</advisory>


<advisory name=”error_text”>
<text>ERROR_TEXT: During the processing of this email an error occurred.
For more information please contact your Symantec(r) representative.
</text>
</advisory>


<advisory name=”error_html”>
<text>
<![CDATA[
<HTML>
<BODY>
<P>ERROR_HTML: During the processing of this email an error occurred.
For more information please contact your Symantec&#174; representative.<BR>
<BR>
<BR>
</P>
</BODY>
</HTML>
]]>
</text>
```

```
</advisory>


<advisory name=”sender_text”>
<text>

The message you sent has been processed by Brightmail(r) AntiVirus
using Symantec’s AntiVirus Technology.

<t name=”file_actions”/>

You may want to install or update antivirus software on your computer.
For more information on antivirus tips and technology, visit
http://www.brightmail.com/antivirus

Headers of infected message:

<t name=”message_headers”/>

</text>
</advisory>


<advisory name=”sender_html”>
<text>
<![CDATA[
<HTML>
<BODY>
<P>
The message you sent has been processed by <b>Brightmail&#174;
AntiVirus</b><BR>
using Symantec’s AntiVirus Technology.<BR>
<BR>
<PRE>
]]>
<t name=”file_actions”/>
<![CDATA[
</PRE>
<BR>You may want to install or update antivirus software on your
   computer.<br>
For more information on antivirus tips and technology, visit
<A HREF=”http://www.brightmail.com/antivirus”>
http://www.brightmail.com/antivirus</A>.<BR>
<BR>
</P>

<p>
Headers of infected message:

<PRE>
]]>

<t name=”message_headers”/>
```

```
<![CDATA[
</PRE>

</BODY>
</HTML>
]]>


</text>
</advisory>


</advisory-list>
```

Glossary

Allowed Senders List – *See Filters*.

AntiSpam Filters – *See Filters*.

AntiVirus Cleaner – The *AntiVirus Cleaner* receives messages from the *Brightmail® Server.* The Cleaner parses the message, decodes most attachments, and cleans them using the Symantec AntiVirus engines and definitions. It then adds a header and message text advising the recipient of its actions, and returns the message via SMTP to the incoming mail stream. The *AntiVirus Cleaner* resides on each *Brightmail Scanner* that includes a *Brightmail Server.* AntiVirus filtering is separately licensed.

AntiVirus Filters – *See Filters*.

Blocked Sender – A sender identified as blocked, either by email address or originating IP address, on the *Blocked Senders List*, on one of the *Brightmail Reputation Service* lists or on a third party blocked senders list. You can configure how messages from blocked senders are handled.

Blocked Senders List – *See Filters*.

BLOC™ – *See Brightmail Logistics and Operations Center.*

bmifilter – *See Brightmail Filter.*

Brightmail Agent – The *Brightmail Agent* resides on each *Brightmail Scanner* and communicates with the *Brightmail Control Center* to support centralized configuration and administration activities.

Brightmail AntiSpam – *See Symantec Brightmail AntiSpam.*

Brightmail Client – The *Brightmail Client* receives messages from the MTA and communicates with the *Brightmail Server* to provide message filtering. The *Brightmail Client* resides on a *Brightmail Scanner.*

Brightmail Control Center – The *Brightmail Control Center* is a Web-based cross-platform configuration and administration center built in Java. Each *Symantec Brightmail AntiSpam* installation has one *Brightmail Control Center*, which also houses *Brightmail*

Quarantine and supporting software. You can configure and monitor all of your Brightmail Scanners from the Control Center. The *Brightmail Control Center* replaces the Brightmail configuration file, the Configurator and the Brightmail Administration Console. These components are no longer included in *Brightmail AntiSpam*.

Brightmail Domino Agent – See Symantec Spam Folder Agent for Domino

Brightmail Filter – (UNIX only) The *Brightmail Filter* allows the Brightmail software to integrate with Sendmail. The *Brightmail Filter* uses the Sendmail Mail Filter API (Milter) to establish a communication stream with Sendmail.

Brightmail Logistics and Operations Center (BLOC) – The *BLOC* is Brightmail's 24/7 spam-fighting facility. Whenever new spam attacks are detected via the *Probe Network*™, the *BLOC* generates new filters to detect and catch the spam, and distributes those filters to all Brightmail Scanners at customer sites. *BLOC* technicians manage and monitor the *BLOC*, and assist in identifying spam.The *BLOC* consists of several centers on three continents, providing round-the-clock protection that spans the globe.

Brightmail Plug-in for Outlook – *See Symantec Plug-in for Outlook.*

Brightmail Quarantine – *Brightmail Quarantine* provides users with Web access to spam messages that the Brightmail software has quarantined for them. Users can browse, search, and delete their spam messages and can also redeliver misidentified messages to their standard inbox. An administrator account provides access to all quarantined messages.

Brightmail Reputation Service – The *Brightmail Reputation Service* provides comprehensive reputation tracking that enhances the power of *Symantec Brightmail AntiSpam*. Brightmail manages three lists as part of the *Brightmail Reputation Service*. Each of these lists operates automatically and filters your messages using the same technology as Brightmail's other filters. The *Brightmail Reputation Service* includes the *Open Proxy List*, the *Safe List* and the *Suspect List*.

- The *Open Proxy List* is a dynamic database containing IP addresses of identity-masking relays, including proxy servers with open or insecure ports. Because open proxy servers allow spammers to conceal their identities and off-load the cost of emailing to other parties, spammers will continually misuse a vulnerable server until it is brought offline or secured.
- The *Safe List* is a list of IP addresses from which virtually no outgoing email is spam.
- The *Suspect List* is a list of IP addresses from which virtually all of the outgoing email is spam.

Brightmail Scanner – Brightmail Scanners are the part of the Brightmail software that performs email filtering. You can have one or many Brightmail Scanners in your *Symantec Brightmail AntiSpam* installation.

Brightmail Server – The *Brightmail Server* filters messages and assigns verdicts to messages based on the filtering results. The *Brightmail Server* resides on a computer hosting a *Brightmail Scanner.*

CIDR – Classless Inter-Domain Routing is a way of specifying a range of addresses using an arbitrary number of bits. For instance, a CIDR specification of 206.13.1.48/25 would include any address in which the first 25 bits of the address matched the first 25 bits of 206.13.1.48.

Company-specific content – You can create custom *Content Filters* that scan messages for *company-specific content*, which you define for your organization. You can specify how messages containing company-specific content are handled.

Conduit – The *Conduit* retrieves new and updated filters from the *BLOC* through secure HTTPS file transfer. Once retrieved, the *Conduit* authenticates filters, and then alerts the *Brightmail Server* that new filters are to be received and implemented. Finally, the *Conduit* manages statistics for use by the *BLOC* and for generating local spam reports. The *Conduit* resides on each *Brightmail Scanner* that includes a *Brightmail Server.*

Content Filters – *See Filters*.

Custom Filters – *See Filters*.

Delivery MTA – A mail server that transfers email to local mail delivery agents (MDAs).

Downstream – A *downstream* mail server is a mail server that receives messages at a later time than other mail servers. In a multiple-server system, inbound mail travels a path from upstream mail servers to downstream mail servers.

False Positive – A piece of legitimate email that is mistaken for *spam* and classified as spam by *Symantec Brightmail AntiSpam*.

Filters – *Brightmail AntiSpam* uses both filters provided by Brightmail and filters provided by customers. *AntiSpam Filters* and *AntiVirus Filters* are sent from the *BLOC*. *Content Filters*, the *Allowed Senders List* and the *Blocked Senders List* are provided by you. Each filter consists of a set of criteria that determine what messages will be filtered. You can set specific actions to be taken on messages found by each type of filter.

- *AntiSpam Filters* are created by the *BLOC* on the basis of information gathered from the Probe Network. These filters use Brightmail's state-of-the-art technologies and strategies to filter and classify email as it enters your site. The *BLOC* then transmits them to all *Brightmail Servers*.
- *AntiVirus Filters* combine Brightmail processing technology with Symantec AntiVirus definitions and engines to clean viruses from your email. The *BLOC* transmits them to all Brightmail Servers. AntiVirus filtering is separately licensed.
- *Content Filters* are written by you to supplement AntiSpam Filters with filters tailored specifically to the needs of your organization. You can use the Custom Filters Editor in the *Brightmail Control Center*, or you can write filters directly in the Sieve language.

- *Allowed Senders List, Blocked Senders List:* The Allowed Senders List and the Blocked Senders List filter messages based on the sender. You can create your own lists and you can subscribe to third-party lists. As a part of Brightmail AntiSpam, you are automatically subscribed to the *Brightmail Reputation Service*, which includes our *Open Proxy List*, *Safe List* and *Suspect List.*

Group Policies – *Group Policies* allow you to specify groups of users, identified by email addresses or domain names, and to customize message filtering for each group. You can add group policies, add users to group policies, and specify the message handling actions for each group policy.

Harvester – The *Harvester* collects mail sidelined by the *Brightmail Server* and transfers it to an SMTP server, which can then take a variety of actions, based upon your configuration choices. The *Harvester* resides on each *Brightmail Scanner* that includes a *Brightmail Server.*

Header – *1*. First part of an email message, containing information such as the address of the recipient, the address of the sender, message type, routing, and time sent. *2*. The `header` test command, a Sieve command supported by the custom filtering features in *Brightmail AntiSpam*.

Installation Directory – (Formerly known as *Load Point*) The directory into which Brightmail software is installed. Also known as the *base directory,* it contains key portions of the Brightmail software, including any daemons, `cron` jobs or utilities running on your Brightmail Server. For UNIX, the default *Installation Directory* is: `/opt/brightmail` for the *Brightmail Scanner*, and `/opt/brightmail/ControlCenter` for the *Brightmail Control Center.* For Windows, the default Installation Directory is `C:\Program Files\Brightmail` for the *Brightmail Scanner,* and `C:\Program Files\Brightmail\ControlCenter` for the *Brightmail Control Center.*

ISP – Internet Service Provider. A company that specializes in providing connections to the Internet, including Web access and email accounts.

Kicker – (UNIX only) The Kicker facility alerts the *Brightmail Server* that new filters are available. The Kicker allows the *Brightmail Server* to be updated without stopping and restarting the *Brightmail Server.*

LDAP – Lightweight Directory Access Protocol, a network protocol for storing, communicating, and validating user address and identification information. LDAP gives users a single tool to comb through data to find a particular piece of information, such as a user name, email address, security certificate, or other information.

LDIF – *LDAP* Data Interchange Format, an Internet Engineering Task Force (IETF) draft format that is a de facto standard for representing directory information in a flat file.

Load Point – *See Installation Directory.*

Mail clients – Also known as MUAs (mail user agents). Programs like the Netscape mail reader and Eudora that enable users to view and edit email messages and folders.

Mass-mailing worm – A worm that propagates itself to other systems via email, often by using the address book of an email client program. See also *worm*.

MDA – Message Delivery Agent, a general term for a program that delivers mail.

MDN – Message Disposition Notification, an internet protocol specifying the contents of specific types of internet email messages. For complete details, refer to RFC2298, An Extensible Message Format for Message Disposition at http://www.faqs.org/rfcs/rfc2298.html.

Messaging Gateway – The outermost point in a network where mail servers are located. All other mail servers are *downstream* from the mail servers located at the *messaging gateway.*

MIME – Multipurpose Internet Mail Extension, a file-type definition standard that enables different mail programs to understand and interpret non-textual file types (such as .doc, .jpg, and .wav) in the same way.

MTA – Mail Transfer Agent, a generic term for programs such as Sendmail or qmail that send and receive mail between servers.

Notifier – Part of *Brightmail Quarantine*, the *Notifier* sends periodic email messages to users, providing a digest of their gray mail. The *Notifier* message is customizable; it can contain a list of the subject lines and senders of all messages suspected to be spam.

Open Proxy List – *See Brightmail Reputation Service*.

Policies – *See Group Policies.*

POP3 – Post Office Protocol version 3, a server/client protocol used to transfer remote mail from a server to a client. Programs like the Netscape mail reader or Eudora can use this protocol to retrieve email from POP servers.

Probe Accounts – Email addresses assigned to Brightmail by our *Probe Network Partners*, and used by *Brightmail AntiSpam* to detect spam.

Probe Network™ – The entire installed base of email accounts provided by Brightmail's *Probe Network Partners*. Used by *Brightmail AntiSpam* for the detection of *spam*, the *Probe Network* has a statistical reach of over 300 million email addresses, and includes over 2 million *Probe Accounts*.

Probe Network Partners – ISPs or corporations that participate in the *Probe Network*.

Quarantine – *See Brightmail Quarantine.*

Relay MTA – A mail server primarily used to transfer email between other mail servers.

Runner – (UNIX only) A job control shell used to start, stop, monitor, and generate diagnostics on Brightmail software operations.

runner.cfg – (UNIX only) The configuration file for the Runner.

Safe List – *See Brightmail Reputation Service.*

Sieve – A language designed for developing email processing applications. The Brightmail software uses this language, including special extensions of the language created by Brightmail, to support custom filtering actions.

SMTP – Simple Mail Transfer Protocol, a server-to-server mail transfer protocol used by many mail systems, such as Sendmail. It is based on TCP/IP.

Spam – Unwanted, unsolicited commercial bulk email. *Symantec Brightmail AntiSpam* uses the term *spam* to identify messages that are determined to be spam, according to its filters.

Spam Folder Agent – The Spam Folder Agent is designed to work on Microsoft Exchange Servers. Installed separately from the standard Brightmail installation, this agent creates a subfolder and a server-side filter in each user's mailbox. The filter gets applied to messages that the *Brightmail Scanner* identifies as spam, routing spam into each user's spam folder, relieving end users and administrators of the burden of using their mail clients to create filters.

Spam Scoring – *Brightmail AntiSpam* assigns a spam score to each message that expresses the likelihood that the message is actually spam. See also *Suspected Spam.*

Spool – A location (directory, file, or database) for storing data temporarily while it is being transferred between devices.

SSR – Symantec Security Response (SSR), a team of intrusion experts, security engineers, virus hunters, and global technical support teams at Symantec Corporation. Analogous to the *BLOC*, SSR provides up-to-date virus definitions and engines to rid email attachments of unwanted viruses.

Suspect List – *See Brightmail Reputation Service*.

Suspected Spam – You can use the *Brightmail Control Center* to define a separate category of messages, called *suspected spam*, based upon *spam scoring*. You can specify different actions for spam messages and suspected spam messages.

Symantec Brightmail AntiSpam – Symantec's system for spam detection and filtering. This includes the *Brightmail Probe Network*, the *BLOC*, filters, the *Brightmail Control Center* and the *Brightmail Scanner.*

Symantec Plug-in for Outlook – The *Symantec Plug-in for Outlook* makes it easy for Outlook users to submit missed spam and false positives to Symantec. Depending on how you configure the plug-in, user submissions can also be sent automatically to a local system administrator. The *Symantec Plug-in for Outlook* also gives users the option to administer their own allowed senders and blocked senders lists.

Symantec Spam Folder Agent for Domino – The Symantec Spam Folder Agent for Domino is an application designed to work with Lotus Domino. Installed separately from

the standard Brightmail installation, the *Brightmail Domino Agent* creates a subfolder and a server-side filter in each user's mailbox. This filter gets applied to messages that the *Brightmail Scanner* identifies as spam, routing spam into each user's spam folder, relieving end users and administrators of the burden of using their mail clients to create filters. The *Brightmail Domino Agent* also allows users to submit missed spam and false positives to Brightmail.

Trojan Horse – A destructive program disguised as a game, utility, or application. When run, the Trojan horse does something harmful to the computer system while appearing to do something useful.

Unscannable – A message is *unscannable* for viruses if it exceeds either the maximum file size or maximum scan depth configured on the **AntiVirus Settings** page on the **Settings** tab. Compound messages such as zip files that contain many levels may exceed the maximum scan depth. You can configure how unscannable messages are handled.

Virus – A program or code that replicates; that is, infects another program, boot sector, partition sector, or document that supports macros, by inserting itself or attaching itself to that medium.

Worm – Self-replicating virus that does not alter files but resides in active memory and duplicates itself. Most worms are spread as attachments to emails. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.

Index

A

Accessing Quarantine 90
Actions and verdicts 37
Active Directory configuration for Quarantine 79
Add
  administrators 15
  Brightmail Scanner 21
  group policy 33
  new member to group policy 35
  senders to your allowed senders list 46
  senders to your Blocked Senders List 45
Adjusting AntiVirus settings 54
Adjusting spam scoring 51
Administering Quarantine 110
Administrator
  add 15
  message details page 93
  message list page 90
Administrator-only Quarantine access 102
Adult content interception 135
Agent, see Brightmail Agent
Alerts, setting up event-based 121
Allowed and Blocked Senders lists
  about 42
  cases for lists 43
  reasons to use Blocked Senders 43
AntiSpam filters 8
Attachments 94, 99
Automatic expansion of subdomains 44

B

Backing up
  all Brightmail data simultaneously 125
  configuration data 124
  logs data 124
  MySQL data 122
  Quarantine data 125
  reports data 124
Blocked and Allowed Senders Lists, see Allowed and Blocked Senders lists.
Body command 132
Brightmail Agent 5
Brightmail AntiSpam
  architecture overview 3
  components 6
  identifies senders and connections 44
  monitoring 117
  overview 1, 4
  starting 31
  stopping 31
  verdicts 37
  version 6.0 enhancements 2
  what's new 2
Brightmail Client 5
Brightmail Conduit 11
Brightmail Control Center 5
  getting started 13
Brightmail Control Center and Brightmail Scanners 20
Brightmail filters 8
Brightmail Quarantine 5, 11
Brightmail Reputation Service 50
Brightmail Scanner 4
  about 19
  delete 25
  disabling 24
  editing configuration 24
  enabling 24
  managing 19
  status information 29
  testing 24
  viewing status 29

Brightmail Server 5
Brightmaillog.log 112

C

Chain letter interception 137
Checking
  Quarantine error log 112
  Quarantine postmaster mailbox 111
  software versions 126
  status of the MySQL database 126
Choosing
  data to track 73
  notification format 105
  required components 22
Cleaner notification file customization 139
Cleaner notification file listing 141
Components, about 19
Configuration backup 124
Configure
  anti-virus filtering 55
  Brightmail Clients 23
  Brightmail Servers 22
  deleting unresolved email setting 107
  global catalog to work With quarantine 82
  login help 108
  messages Per Page in Quarantine 108
  Quarantine 101
  Quarantine for Active Directory 79
  Quarantine for administrator-only access 102
  Quarantine for Exchange 5.5 83
  Quarantine for iPlanet/Sun ONE/Java Directory 85
  Quarantine for other LDAP servers 88
  Quarantine port for incoming SMTP email 109
  Quarantine settings 92, 94
  recipients for misidentified messages 106
  spam scoring 51
  user and distribution list notification digests 102
Connections from server to client 23
Content filters 9
Create
  conditions in custom filters 58
  custom filters 56
  filters by coding in the sieve language 129
  new group policy 33
  reports 69
Custom filtering
  components 58
  details about 64
  disabling 64
  editing 56
  enabling 64
  importing a custom filters file 64
  samples 65
  tests 60
Customizing
  Brightmail Reputation Service 50
  Cleaner notification file 139
  filtering at your site 41

D

Data backup 125
  configuration 124
  logs 124
  MySQL 122
  Quarantine 125
  reports 124
Data retention for report information 76
Decoding headers 130
Define
  filtering actions for new group policy 37
  initial host configuration 21
Delete
  all Quarantine messages 91, 97
  Brightmail Scanners 25
  filters 63
  group policy 40
  group policy member 35
  individual Quarantine messages 91, 97
  senders from lists 47
  unresolved email setting 107
Delivering messages to Quarantine from the Brightmail Server 101
Determining
  filter order 63
  fully qualified domain names on Windows 82
  netbios names on Windows 82
Differences
  between the administrator and user message list pages 92
  between the administrator and user message pages 94
  between the administrator and user search pages 96
Disable
  Brightmail Scanners 24
  filters 64
  group policy 40

senders 47
Disk space maintenance 125
Displaying full or brief headers 93, 99
Does not match test 60
Domain names, Windows 82
Double-counting of virus messages 76
Duplicate messages in Quarantine 115

E

Edit
Brightmail Scanner configuration 24
existing group policy 39
filters 62
senders 47
virus notification messages 139
Edit, see also configure.
Email handling verdicts and available actions 37
Enable
Brightmail Scanners 24
data tracking for reports 73
filters 64
group policy 40
language identification 53
notification for distribution lists 105
senders 47
Encoded headers decoded 130
Envelope command 133
Error in Quarantine log file from no disk space or full work directory 115
Error in Quarantine log file from very large spam messages 114
Example values for Allowed Senders list 46
Exchange 5.5 directory information 83
Exchange 5.5 settings for Quarantine compatibility 83
Export group policy members to file 37
Export sender information 50

F

File containing Sieve filters 130
Filter components 58
Filter order determination 63
Filter tests 60
Foldering submissions 11
Frequency of digest notification 103
Full administrative privileges 15

G

Gateway deployment 20
Global catalog configuration 82
Glossary of terms 147
Graphics appear as gray rectangles 94, 99
Greeting card interception 137
Group policies, email categories and filtering actions 6
Group policy
add 33
delete 40
delete a member from 35
disable 40
edit existing 39
enable 40
managing 39

H

Header decoding 130
Header, displaying full or brief 93, 99
Helo domain 138
Hosts, about 19

I

Import
custom filters file 64
group policy members from file 35
sender information 48
Insertion host specification 25
Intercept
adult content 135
chain letters 137
for size 66
greeting cards 137
MIME type 67
sender or recipient 67
senders, based on the HELO domain 138
specified virus 137
Internal IP address specification 26
Internal mail host addresses 27
iPlanet/Sun ONE directory server access 86

K

Keep command 131

L

Language identification, define languages to

filter 53
Large message interception 66
LDAP
server alternate access 88
server configuration 79, 88
License expiration 126
Log
backing up 124
Increasing amount of logging information in Brightmaillog.log 112
manage 15
modifying settings 118
Quarantine error log, Checking 112
restore tables 125
Save 125
saving 120
tables 125
view for Brightmail Scanner 120
viewing 120
working with 118
Log backup 124
Logical connections and internal mail servers, non-Gateway Deployments 45
Login problems 113
Login steps 13
Logout steps 14

M

Maintenance
disk space 125
system 122
Maintenance of the system, periodic 122
Manage
group policies 16, 33, 39
Quarantine 15, 16
reports 16
Scanners, hosts and components 19
status and logs 15
Match and Does Not Match tests 60
Matched 131
Maximum number of Quarantine messages 116
Message
”the operation could not be performed.” is displayed 113
delivery statistics 76
details page 98
interception based on MIME type 67
interception based on sender/recipient 67
interception based on size 66
list page 96
list page details 98
MIME-based message interception 67
Mimeheader command 134
Modifying log settings 118
Monitoring Brightmail AntiSpam 117
MySQL
backup 124
data backup 122
database status 126

N

Navigating through messages 91, 93, 97, 99
Nesting if-then statements 129
Netbios names on Windows 82
New in Brightmail AntiSpam 2
Notification for distribution lists/aliases 102
Notification message variables 104
Notify us of potential missed spam 11

P

Periodic system maintenance 122
Printing reports 77
Procedure to
add a new member to this group policy 35
add an administrator 16
add email addresses, domains, and third-party lists to Allowed Senders list 46
add email addresses, domains, and third-party lists to your Blocked Senders list 45
adjust the spam score for suspected spam 52
change the notification digest frequency 103
change the order by which filters are checked 63
choose a notification format 105
configure AntiVirus filtering 55
configure Quarantine for administrator-only access 102
configure Quarantine to access Active Directory 79
configure Quarantine to access an alternate LDAP Server 88
configure Quarantine to access Exchange 5.5 directory information 83
configure Quarantine to access iPlanet/Sun ONE Directory Server 86
configure recipients for misidentified message submissions 106
configure the Brightmail Server 23

create a new group policy 33
create custom filters 57
define filtering actions for new group policy 37
delete a Brightmail Scanner 25
delete a filter from the list 63
delete a group policy 40
delete a group policy member 35
delete a scheduled report 78
delete senders from your Blocked Senders list or Allowed Senders list 47
deliver messages to Quarantine 101
determine the NetBIOS name for your Active Directory domains 82
disable a group policy 40
display messages sent to the postmaster mailbox 111
edit a Brightmail Scanner 24
edit a filter in the list 62
edit a scheduled report 78
edit an existing group policy 39
edit senders in Blocked or Allowed Senders list 47
edit the notification templates, digest subject, and send from address 104
enable a group policy 40
enable data tracking for reports 73
enable language identification 53
enable or disable a Brightmail Scanner 24
enable or disable filters in custom filters list 64
enable or disable senders from your lists 48
export group policy members to a file 37
export sender information from Blocked Senders or Allowed Senders list 50
grant permission to the current domain controller 83
import a custom filters file 64
import group policy members from a file 35
import sender information from allowed-blockedlist.txt file 50
modify contents of existing login help page 108
modify log settings for a Brightmail Scanner 118
replicate the NCName attribute to the Global Catalog with Active Directory Schema snap-in 82
restore configuration tables from backup 124
restore Quarantine tables from backup 125
restore the Brightmail database from backup 125
restore the Logs tables from backup 125
restore the Reports tables from backup 124
run a report 73
run the MySQL verify/repair scripts 126
save a report 76
save Quarantine tables 125
save the Brightmail database 125
save the configuration tables 124
save the Logs tables 125
save the Reports tables 124
schedule a report 77
select lists in Brightmail Reputation Service 51
set group policy precedence 39
set the number of messages displayed per page 108
set the Quarantine Message Retention Period 107
set up a Brightmail Scanner 21
set up alerts 121
set up Brightmail Server connections for Brightmail Clients 23
specify a custom Login help page 108
specify how long Brightmail AntiSpam saves report data 72
specify Quarantine message and size thresholds 109
specify the addresses for internal mail hosts 27
specify the components to enable on a Brightmail Scanner 22
specify the insertion host for a Brightmail Scanner 25
start Quarantine processes on UNIX 110
start Quarantine services on Windows 111
stop Quarantine processes on UNIX 110
stop Quarantine services on Windows 111
test a Brightmail Scanner 24
view group policy information for user or domain 40
view the status of Brightmail Scanners and components 30

Q

Quarantine
access administrator-only configuration 102
administrator-only access 102
configuration 101
configuration for Active Directory 79
data backup 125
distribution lists and aliases 102
duplicate messages 115
for Exchange 5.5 configuration 83
for iPlanet/Sun ONE/Java Directory Server

configuration 85
for LDAP server configuration 88
global catalog configuration 82
LDAP for end user access 79
LDAP Server alternate access 88
log file error for no disk or directory space 115
log file error from very large spam messages 114
message navigation 91, 93, 97, 99
message redelivery 91, 93, 97
message retention, setting 107
message sorting 90, 97
messages per page configuration 108
messages, maximum allowed 116
port for SMTP email configuration 109
searching details 95, 100
size and message thresholds 109
Stopping and Starting 110
table restore 125
tables, saving 125
thresholds 109

R

Redelivering misidentified messages 91, 93, 97, 98
Report
available types 69
basis of message statistics 76
creating 69
data backup 124
data tracking 73
deletion 78
double-counting virus messages 76
editing scheduled report 78
enable data tracking 73
limitation of report size 76
limited to 1,000 rows 76
presentation 75
printing 77
retention 72, 76
run 73
save 76
schedule 77
size limitations 76
tables 124
tables, save 124
time shown for data 75
troubleshooting report generation 74
Reputation Service customization 50
Restart requirements after editing script 129
Restore 124
Brightmail database 125
configuration tables 124
logs tables 125
Quarantine tables 125
Retention of report data 76
Returning to the message list 93, 99
Run
report 73
scripts to verify and/or repair MySQL problems 126

S

Sample
custom filters 65
values for blocked senders lists 45
Save 125
Brightmail database 125
configuration tables 124
Quarantine tables 125
reports tables 124
Saving reports 76
Scanner, See also Brightmail Scanner.
Scheduling reports 77
Scripts for MySQL, how to run 126
Search, details 95, 100
Searching
“From” Headers 95, 100
“To” Headers 94
Message ID header 95, 100
messages 91, 94, 97, 99
subject headers 95, 100
using Multiple Characteristics 94, 99
using Time Range 95, 100
Selecting the notification digest format 105
Sender interception 138
Senders
disabling 47
enabling 47
Separate notification templates for standard and distribution list messages 103
Server connections for Clients 23
Set
alerts 121
Brightmail Scanners 20
event-based alerts 121
group policy precedence 39
Quarantine message retention period 107
retention period for reporting data 72
size limit on incoming mail 137

Settings, available 54
Sieve
  Action commands 131
  action Precedence 135
  changing the filters file 129
  execution termination 130
  filters file Location 130
  implementation details 130
  manually edited filters 129
  matched 131
  statement nesting 129
  supported commands 130
  Test Commands 132
Sieve commands
  Body 132
  Envelope 133
  Keep 131
  Mimeheader 134
Sieve language coding 129
Sieve script, restart requirements 129
SMTP insertion host specification 25
Software versions 126
Sorting messages 90, 97
Spam foldering and submissions 11
Spam reports 70
Specifying
  Allowed and Blocked Senders 41
  internal mail hosts 26
  Quarantine message and size thresholds 109
  SMTP insertion host 25
Starting and stopping Brightmail AntiSpam 31
Starting and stopping Quarantine 110
Status
  information for Brightmail Scanners and components 29
  MySQL database 126
  system 117
Subdomain expansion 44
Submitting email to us you didn't want 11
Summary tab items 117
Sun ONE directory server access 86
Supported methods for identifying senders 44
Supported sieve commands 130
Syntax for preparing importable list for Allowed and Blocked Senders 49
System maintenance 122
System status 117

T

Terminate execution promptly 130
Testing Brightmail Scanners 24
Tests for matching 60
Third party software
  database, Web server 5
Threshold specification for Quarantine 109
Time displayed on reports 75
Tracking report data 73
Troubleshooting
  login problems 14
  Quarantine 113
  report generation 74

U

Undeliverable Quarantined messages 114

V

Verdicts from Brightmail AntiSpam 37
Version, how to check 126
View
  Brightmail Scanner logs 120
  group policy information for user or domain group policy 40
  messages 90, 97
  status of Brightmail Scanners and components 29
Viewing and saving logs 120
Virus
  interception 137
  messages double-counting 76
  notification message editing 139
  reports 70

W

What's new in Brightmail AntiSpam 2
White space 130
Wildcards in matches 60